View Manager 管理指南

View Manager 4.0.1

在新版文档推出之前，本文档支持所列出的所有产品版本及其所有后续版本。要查看本文档的最新版本，请参见 http://www.vmware.com/cn/support/pubs。

CN-000242-02

您可在 VMware 网站中找到最新技术文档：

http://www.vmware.com/cn/support/

VMware 网站还提供了最新产品更新。

如果对本文档有任何意见或建议，请将反馈信息提交至以下地址：

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware Global, Inc.
北京办公室 北京市海淀区科学院南路 2 号融科资讯中心 C 座 8 层
邮编：100190 电话：+86-10-5993-4310 或 5993-4306
上海办公室 上海市徐汇区淮海中路1010号嘉华中心27楼2720-2721室
邮编：200031 电话：+86-21-6103-1234
广州办公室 广州市天河北路 233 号中信广场 7401 室
邮编：510613 电话：+86-20-3877-1938
http://www.vmware.com/cn

目录

关于本书

本管理指南讲述如何安装、配置和使用 VMware® View™，其中包括如何安装不同的软件组件、如何部署服务器、如何部署桌面和控制用户访问。本指南还讲述了客户端软件，这种客户端软件可将用户连接到 VMware vSphere™ 中运行的虚拟桌面中，也可连接到您的网络环境内运行的物理系统。

本章将讲述以下主题：

- 第 9 页上的 "目标读者"
- 第 9 页上的 "文档反馈意见"
- 第 10 页上的 "技术支持和培训资源"

目标读者

本书适用于需要安装、管理或配置 View Manager 的用户。本指南中的信息专门为已熟练掌握虚拟机技术和数据中心操作、且具有丰富经验的 Windows 或 Linux 系统管理员编写。

文档反馈意见

VMware 欢迎您提供文档改进意见和建议。如有任何意见或建议，请将反馈信息提交至以下地址：docfeedback@vmware.com

技术支持和培训资源

以下部分列出了您可利用的技术支持资源。要获取本书以及其他书籍的最新版本，请访问 http://www.vmware.com/cn/support/pubs。

联机支持和电话支持

要使用联机支持提交您的技术支持请求，请查看产品及合同信息并注册产品，然后访问 http://www.vmware.com/cn/support。

对于优先级最高的问题，已签署相应支持合同的客户应使用电话支持，以最快地获得支持。请访问 http://www.vmware.com/cn/support/phone_support。

支持服务

了解 VMware 支持服务如何帮助满足您的业务需求，请访问 http://www.vmware.com/cn/support/services。

VMware 专业服务

VMware 培训服务课程提供了丰富的实践练习、案例研究示例和课程材料，可用作您工作中的参考工具。培训形式多样，包括现场授课、课堂培训以及实时网络教学。对于现场指导项目和最佳操作方法， VMware 咨询服务提供了多种服务，帮助您评估、规划、构建和管理您的虚拟环境。要获取有关培训课程、认证计划以及咨询服务的信息，请访问 http://www.vmware.com/cn/services。

简介 1

View Manager 是一款灵活而直观的桌面管理解决方案，可让系统管理员快速地部署桌面并控制用户的访问权限。该客户端软件可将用户连接到 VMware vSphere 中运行的虚拟桌面，也可连接到用户网络环境中运行的物理系统。

本章概述 View Manager 的主要功能，并介绍安装和运行此应用程序相关软件组件时所需满足的系统要求。

本章讲述以下主题：

- 第 11 页上的 "View Manager 概述"
- 第 14 页上的 "View Manager 组件"
- 第 14 页上的 "系统要求"

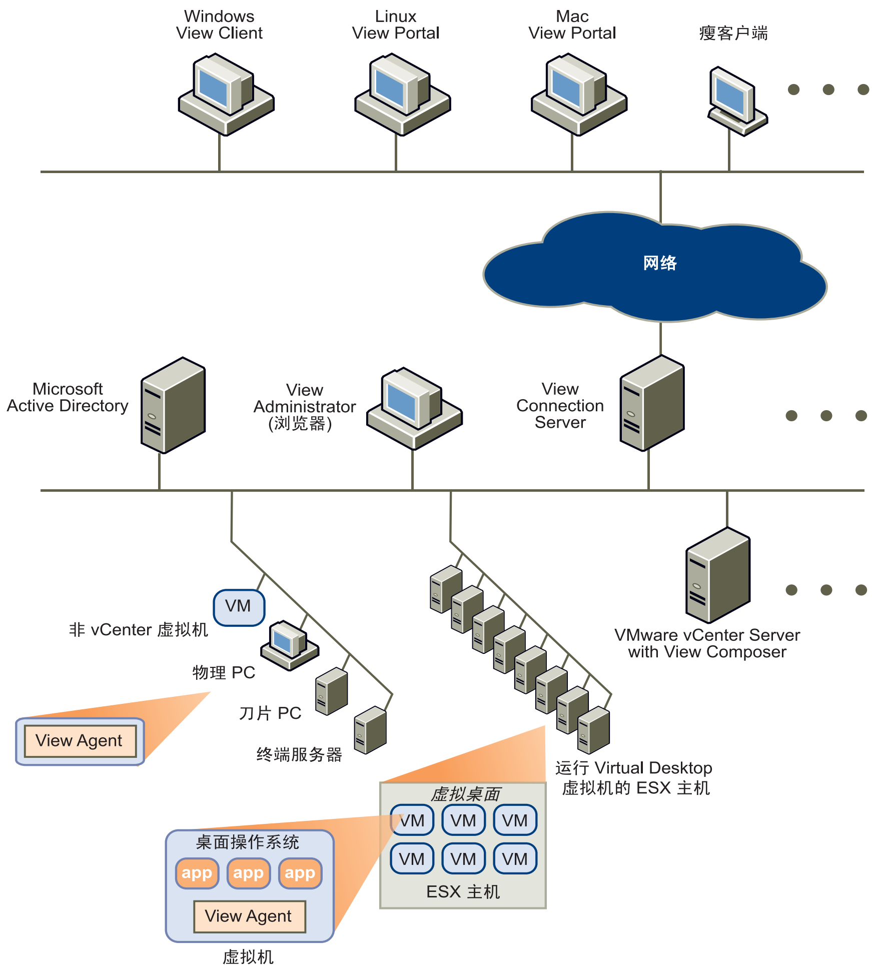
View Manager 概述

View Manager 与 VMware vCenter Server 紧密集成，允许管理员从 VMware ESX 上运行的虚拟机中创建桌面，然后部署桌面至最终用户。此外， View Manager 还可充分利用您现有的 Active Directory 基础架构对用户进行身份验证和管理。

创建桌面之后，使用基于 Web 或本地安装的客户端软件，经授权的最终用户可以安全连接到集中化的虚拟桌面、后端物理系统或终端服务器。

图 1-1 以 View Manager 环境为例，显示其高级视图和主要组件。稍后，我们将在本书的后续章节详细介绍这些组件。

图 1-1. View Manager 环境中的高级视图



View Manager 的主要功能

View Manager 具有以下几大主要功能：

- 企业级的连接代理 － View Manager 可管理用户与其虚拟桌面之间的连接。当用户与 View Manager 相连时，系统随即显示该用户有权访问的虚拟桌面。
- "智能桌面池" 功能 － 提供各种永久型和非永久型桌面池功能，可以简化集中式桌面的部署与管理。
- 灵活的部署选项 － View Manager 组件可以采用各种配置进行部署，并可部署至网络的不同部分，从而显著提高安全性、伸缩性和可靠性。此外， View Manager 还支持多台 vCenter Server，并可水平缩放以支持多个虚拟桌面。
- 高可用性 － View Manager 具有自动故障切换功能，可通过建立 View Manager Server 集群，实现高可用性和伸缩性。此外，这些服务器还可充分利用业内标准的负载平衡解决方案。
- 与 Microsoft Active Directory 完美集成 － View Manager 可与 Active Directory 相连，允许您定位用户及用户组的帐户，并使用身份验证功能控制哪些用户可以访问虚拟桌面。
- 与 VMware vSphere 无缝集成 － View Manager 与 VMware vCenter Server 集成运行，可提供许多高级虚拟桌面管理功能 （例如，自动挂起和恢复），从而显著减少托管虚拟桌面所需的内存和处理能力。

  通过利用 VMware vSphere 的强大功能，即使服务器硬件出现故障桌面仍可正常运行，并可从意外中断中快速恢复，根本无需配备重复的硬件。
- 安全访问 － View Manager 提供了许多可选的安全封装功能，允许对所有网络连接进行加密。
- 支持双因素身份验证 － 凭借 RSA SecurID，访问控制得到了进一步加强。
- USB 客户端设备和虚拟打印支持 － USB 设备和打印机均可本地连接至客户端，但可从虚拟桌面中访问。
- 基于 Web 的管理用户界面 － View Manager 提供一款基于 Web 的管理控制台，允许从任何位置管理虚拟桌面。
- 支持非 vSphere 系统 － View Manager 还可管理物理机或终端服务系统，从而确保现有体系结构无缝集成至 View 环境中。
- 可伸缩的虚拟基础架构 － View Manager 采用链接克隆技术，支持从一个基础映像部署多个桌面。对此映像的任何后续更改都将自动传播至链接克隆池中的所有桌面。
- View Manager 是一款完全国际化的产品。

View Manager 组件

View Manager 包含以下主要组件：

- View Connection Server － 充当客户端连接代理的软件服务，负责进行身份验证并将传入的远程桌面用户请求转到相应的虚拟桌面、物理桌面或终端服务器中。
- View Agent － 安装在所有客户虚拟机、物理系统或终端服务器中的软件服务，旨在允许 View Manager 对它们进行管理。该代理具有很多种功能，例如：连接监控、虚拟打印、 USB 支持以及单点登录等。
- View Client － 安装在本地的软件应用程序，用来与 View Connection Server 进行通信，旨在允许用户连接到桌面。
- View Client with Offline Desktop（处于试验阶段）－ 经过扩展可支持脱机桌面功能的 View Client 版本，允许用户下载虚拟机，并在本地系统中使用。
- View Portal － 基于 Web 的 View Client 版本，支持多种操作系统和浏览器。
- View Administrator － 一种基于 Web 的应用程序，支持 View Manager 管理员配置 View Connection Server、部署和管理桌面、控制用户身份验证、启动并检查系统事件以及执行分析活动。
- View Composer － 安装在 vCenter Server 中的软件服务，支持 View Manager 从一个集中式基础映像中快速部署多个链接克隆桌面。

系统要求

以下部分介绍 View Manager 主要组件的硬件和软件要求。

注释 在部分产品版本中， VMware 提供了一些 “试验性” 和 “技术预览” 功能。这些功能仅供您测试和体验使用。请勿在生产环境中使用。但是，如果您在使用试验性功能或技术预览功能时遇到任何问题，请向我们提供任何反馈意见，我们对此表示衷心的感谢。请通过正常访问方法提交支持请求。您将收到系统自动发出的请求确认邮件。但是，我们无法承诺为这些功能提供疑难解答、解决方法或对其进行修复。

View Connection Server

View Connection Server 在已安装 Windows 终端服务器角色的服务器中不受支持。请从要安装 View Connection Server 的任何服务器中删除 Windows 终端服务器。

View Connection Server 在具有以下规格的 32 位或 64 位专用物理服务器或虚拟服务器中运行：

- 处理器为 Pentium IV 2.0Ghz 或更高版本 – 建议使用双核处理器
- RAM 为 2GB 或更高 – 若要部署 50 或 50 个以上 View Manager 桌面，建议使用 3GB RAM
- 一个或多个 10/100Mbps 网络接口控制器 (NIC) – 建议使用 1Gbps NIC

注释 以上规格适用于为了达到高可用性或外部访问目的而在环境中安装的任何其他 View Connection Server 实例。

支持的操作系统

View Connection Server 可以安装在以下 32 位操作系统中：

- Windows Server 2003 R2 Standard Edition with SP2
- Windows Server 2003 Standard Edition with SP2
- Windows Server 2003 R2 Enterprise Edition with SP2
- Windows Server 2003 Enterprise Edition with SP2

先决条件

View Connection Server 要求以下先决条件：

- 有效的 View Manager 许可证注册码。可选择以下类型的许可证：
  - View Manager
  - 带 View Composer 的 View Manager
  - 带 View Composer 和 Offline Desktop 的 View Manager

- VMware 虚拟化环境
  - VMware vSphere 4 Update 1。必须安装 Update 1。
  - VMware Infrastructure 3.5。建议安装 Update 3 或 Update 4。不支持 Update 5。
  - 支持 VMware Infrastructure 3.0.2。
  - 支持 ESX 和 ESXi 主机。
  - 必须安装 vCenter。

  注释 要使用 View Composer 功能，需要安装 VMware vSphere 4 Update 1 或者 VMware Infrastructure 3.5 Update 3 或 Update 4。

  要使用 Offline Desktop 试验性功能，需要安装 VMware Infrastructure 3.5 Update 3 或 Update 4。 vSphere 4 不支持 Offline Desktop。

- 运行标准或副本 View Connection Server 实例的主机操作系统已加入 Active Directory 域中。支持以下 Active Directory 版本：
  - Windows 2000 Active Directory
  - Windows 2003 Active Directory
  - Windows 2008 Active Directory

  注释 View Connection Server 无需对 Active Directory 的任何方案或配置进行更新。

- 为了在标准 （非链接克隆）桌面池中应用自定义规范，必须在 vCenter Server 中安装 Microsoft Sysprep 工具。

RSA Authentication Manager

View Connection Server 已经过 RSA Authentication Manager 6.1 和 7.1 版本的认证。此外，其他与 6.1 版本兼容的 RSA Authentication Manager 版本也同样支持 View Connection Server。

操作系统对组件安装的支持情况

表 1-1 列出了不同类型的 Windows 操作系统为本地安装的 View Manager 组件提供的支持。对于每款组件，仅提供 32 位支持。在后续章节中，我们将介绍这些组件的其他环境要求。此表中包括以下各列：

- "View Agent"，是指安装在 View Manager 桌面中的 View Agent 服务。此列中的条目表示可由 View Manager 进行管理的操作系统。此列分为两个子列：
  - "虚拟"，是指作为客户机支持的虚拟系统。这些系统既可驻留在 VMware vSphere 内进行部署和管理，也可作为独立系统位于另一 VMware 应用程序（例如， VMware Server）中。
  - "物理"，是指作为多个备选后端支持的物理系统，其中包括终端服务器。
- "View Client"，是指 View Client 应用程序。此列中的条目表示可以安装并运行此应用程序的操作系统。
- "Offline Desktop"，是指 View Client with Offline Desktop 应用程序。此列中的条目表示可以安装并运行此应用程序的操作系统。有关可以在脱机环境中下载并使用的 View Manager 桌面列表，请参阅第 23 页上的 "View Client with Offline Desktop：支持的客户机"。
- "View Composer"，是指在 vCenter Server 主机系统中运行的 View Composer 服务。此列中的条目表示可以运行此服务的操作系统。

注释 此表中未列出 View Connection Server 的要求。有关此组件的详细信息，请参阅第 15 页上的 "View Connection Server"。

表 1-1. 操作系统 （32 位）对组件安装的支持情况

操作系统	View Agent		View Client	Offline Desktop
	虚拟	物理		
Windows 2000 Professional SP4			是	
Windows XP Professional SP2	是	是	是	是
Windows XP Professional SP3	是	是	是	是
Windows XP Home SP2			是	
Windows XP Home SP3			是	
Windows XPe			是	
Windows Vista Home SP2			是	
Windows Vista Business SP1	是	是	是	
Windows Vista Enterprise SP1	是	是		
Windows Vista Business SP2	是	是	是	
Windows Vista Enterprise SP2	是	是	是	
Windows Vista Ultimate SP1	是	是	是	
Windows Vista Ultimate SP2	是	是	是	
Windows 7	技术预览	技术预览	技术预览	
Windows Server 2003 R2 Enterprise Terminal Server	是	是		
Windows Server 2003 Enterprise Terminal Server SP2	是	是		

有关技术预览功能的详细信息，请参阅第 14 页上的 “系统要求”。关于 Windows 7 支持的更多信息，请参阅发行说明。

操作系统对 Web 组件的支持情况

表 1-2 列出了不同类型的操作系统对 View Manager 基于 Web 组件的支持，此外，还列出了特定的浏览器和附加软件要求。在后续章节中，我们将介绍这些基于 Web 组件的任何其他环境要求。

表 1-2. 操作系统对基于 Web 组件的支持情况 （32 位）

操作系统	View Portal	View Administrator
Windows XP Professional SP1	Internet Explorer 6 SP2 Internet Explorer 7	Internet Explorer 7 Internet Explorer 8 Firefox 3.0 Firefox 3.5
Windows XP Professional SP2		
Windows XP Professional SP3		
Windows XP Home SP2		
Windows XP Home SP3		
Windows Vista Home	Internet Explorer 7	
Windows Vista Home Premium		
Windows Vista Business		
Windows Vista Business SP1		
Windows Vista Ultimate		
Windows Vista Ultimate SP1		
RHEL 5.0, Update 1 （处于试验阶段）	Firefox 2.0 / 3.0 Java JRE 1.5.0 或 1.6.0 rdesktop	
SLES 10 SP1 （处于试验阶段）		
Ubuntu 8.04 （处于试验阶段）		
Mac OS/X Tiger （10.4）（处于试验阶段）	Safari Java JRE 1.5.0 RDC 2.0	
Mac OS/X Leopard （10.5）（处于试验阶段）		

View Agent

您必须具有管理权限才能在 Windows View Manager 桌面中安装 View Agent。

View Composer

您无法使用 View Manager 的 View Composer 功能来部署运行 Windows Vista Ultimate Edition 或 Windows XP Professional SP1 的桌面。有关 View Composer 的详细信息，请参阅第 121 页上的第 6 章，"View Composer"。

批量许可证和 Windows Vista Ultimate

Windows Vista Ultimate 并不是为广泛的企业部署而设计的，因此它不支持批量许可证。要部署使用 Windows Vista Ultimate 的桌面克隆，您必须先联系 Microsoft，以确定您的许可限制。

View Client / View Client with Offline Desktop

您必须具有管理权限才能在客户端桌面中安装 View Client 或 View Client with Offline Desktop。要将连接的 USB 设备重定向至 View Manager 桌面中要使用的客户端系统，必须在安装客户端应用程序时启用 USB 重定向功能。

注释 Offline Desktop 是一种试验性功能。有关试验性功能的详细信息，请参阅第 14 页上的 "系统要求"。

vSphere 4 不支持 Offline Desktop。要使用 Offline Desktop 试验性功能，需要安装 VMware Infrastructure 3.5 Update 3 或 Update 4。

智能卡支持

支持使用 PKCS#11 或 Microsoft CryptoAPI 提供程序的智能卡和读卡器。

显示协议

View Client 支持 RDP、 PCoIP 和 HP RGS 显示协议。

PCoIP

PCoIP 为 LAN 或 WAN 中的广大用户提供了交付的整个桌面环境的最佳桌面体验，包括应用程序、图像、音频和视频等。 PCoIP 可弥补因延迟增加或带宽减少导致的不便，确保最终用户在任何网络条件下均可保持高效。PCoIP 可以作为虚拟机和使用 Teradici 主机卡的物理机的 View 桌面的显示协议。

主要功能和限制包括：

- 支持通过虚拟专用网络 (VPN) 进行远程连接。
- 支持表 1-1 中列出的 View Agent 操作系统版本连接到 Windows XP 和 Windows Vista 桌面。
- 支持表 1-1 中列出的 View Client 操作系统版本从 Windows XP 和 Windows Vista 客户端进行连接。
- 使用 PCoIP 的 View Client 可以连接到 View 安全服务器，但与桌面进行的 PCoIP 会话会忽略安全服务器。 PCoIP 使用 UDP 来传输流式音频和视频。安全服务器仅支持 TCP。
- 不支持智能卡。
- 不支持虚拟打印。
- Windows 客户端支持 MMR 重定向。
- 支持 USB 重定向。
- 支持减少 Adobe Flash 带宽。
- 支持音频重定向，可针对 LAN 和 WAN 动态调整音频质量。
- 建议的客户操作系统设置包括：
  - 768 MB RAM 或更多
  - 单 CPU
- 客户端硬件的要求包括：
  - 800 Mhz 或更快的处理器速度
  - 具有 SSE2 扩展指令集、基于 x86 的处理器
  - 有关适用于特定显示器配置的 RAM 大小，请参见 《VMware View 体系结构规划指南》。
- 您最多可以使用四个显示器，并可以分别调整各显示器的分辨率，每个显示器的最大分辨率为 1920x1200。支持旋转显示和自动调整功能。
- 支持用 32 位色彩进行虚拟显示。
- 支持 ClearType 字体。
- 您可以在本地系统和桌面之间复制和粘贴文本，但不能在系统之间复制粘贴系统对象，如文件夹和文件。

远程桌面 (RDP)

建议在 Windows XP 和 Windows XPe 中使用 Microsoft 远程桌面连接 (RDC) 6.x。Windows Vista 已附带安装了 RDC 6.x。您至少安装 RDC 6.0，才能支持多显示器。

您可以点击下面的地址下载 RDC 6.1：

http://microsoft.com/downloads/details.aspx?familyid=6E1EC93D-BDBD-4983-92F7-479E088570AD

对于 Windows XP 桌面虚拟机，请确保安装以下 Microsoft 知识库 （KB）文章引用的 RDP 修补程序：

http://support.microsoft.com/kb/323497

http://support.microsoft.com/kb/884020

如果未安装上述修补程序，则客户端上可能会显示 [Windows Sockets failed error （Windows Socket 失败错误）] 消息。

Windows 2000 不支持 RDC 6.x。支持 RDC 5.0。

HP 远程图像软件 （Remote Graphics Software）

远程图像软件 （Remote Graphic Software， RGS）是一种来自 HP 的显示协议，允许用户通过标准网络访问远程计算机的桌面。支持 HP RGS 5.2.5 版。请与 HP 联系，获得 HP RGS 软件版本 5.2.5 的许可，以与 View 结合使用。 VMware View 未捆绑或许可 HP RGS。

主要功能和限制包括：

- View Client （用于 Windows）支持在连接 HP Blade PC、 HP Workstation 和 HP Blade Workstation 时使用 HP RGS 连接桌面。
- 不支持连接到虚拟机。
- 不支持 Vista 桌面。
- 仅支持直接连接。不支持安全加密链路连接。
- 不支持智能卡。
- 不支持多显示器。
- View Portal 不支持 RGS 连接。
- Linux 瘦客户端不支持 RGS 连接。

产品兼容性

同一台计算机上不能同时安装 View Client、 View Client with Offline Desktop 和 View Agent。

您无法在装有 VMware ACE、 VMware Player、 VMware Server 或 VMware Workstation 的任何系统上安装 View Client with Offline Desktop。在安装 View Client with Offline Desktop 之前，必须卸载上述应用程序。

View Client with Offline Desktop：支持的客户机

可以下载并在 View Client with Offline Desktop 中使用以下 32 位操作系统：

- Windows XP Professional SP2
- Windows XP Professional SP3

View Client 和 View Client with Offline Desktop：MMR

多媒体重定向 (Multimedia Redirection, MMR) 功能使用虚拟通道直接将多媒体流交付到客户端。这样便保证了高保真回放。在 Windows XP、 Windows XP Embedded 和 Windows Vista 客户端操作系统上的 View Client 和 View Client with Offline Desktop 支持 MMR。

请确保将 MMR 端口作为例外情况添加到防火墙软件中。默认端口为 9427。

MMR 支持以下媒体格式：

- AC3
- MP3
- MPEG-1
- MPEG-2
- MPEG-4-part2
- WMA
- WMV 7/8/9

建议使用 Windows Media Player 10 这款应用程序来处理上述文件。此应用程序支持 MMR，且应同时安装在客户端和 View Manager 桌面中。

注释 如果 View Client 视频显示硬件不支持覆盖功能， MMR 将无法正常运行。

View Portal

对于那些在 Internet Explorer 6 或更高版本中使用 View Portal 访问其桌面的 Windows 用户而言，必须安装 ActiveX 控件。

您必须先安装 rdesktop 1.5.0，然后才可使用 Linux 系统中的 View Portal 连接到 Windows 桌面。您可从以下位置下载到 rdesktop：

http://www.rdesktop.org

下载 rdesktop 之后，请按照 `readme` 文件中的说明执行。

操作系统支持

View Portal 在 Mac OS/X 和 Linux 操作系统中尚属于试验性功能。有关试验性功能的更多信息，请参阅第 14 页上的 "系统要求"。

支持 USB

为了使用 View Portal 附带的 USB 重定向功能，用户必须先在本地系统中安装 View Client。有关此操作的详细信息，请参阅第 90 页上的 "安装和运行 View Client 与 View Portal"。

Windows 2000 不支持 USB 重定向。

虚拟打印

View Portal 不支持虚拟打印。

View Composer

View Composer 功能需要靠 VMware 虚拟化环境实现：

- VMware vSphere 4 Update 1
- VMware Infrastructure 3.5 Update 3 或 Update 4。不支持 VMware Infrastructure 3.5 Update 5。

您可以在混合包含了 ESX/ESXi 4 主机和 ESX/ESXi 3.5 主机的群集上部署一个链接克隆桌面池，直到您设置了 **[vSphere]** 模式。

以下 32 位平台支持 View Composer 功能：

- Windows Server 2003 Service Pack 2 或更高版本
- Windows XP Professional Service Pack 2 或更高版本

注释 您无法使用 View Manager 的 View Composer 功能来部署运行 Windows Vista Ultimate Edition 或 Windows XP Professional SP1 的桌面。

数据库要求

要存储 View Composer 数据，则还要求 vCenter Server 上包含 SQL 数据库，或者 vCenter Server 能够使用 SQL 数据库。

注释 如果 vCenter Server 中已存在 SQL 数据库，则 View Composer 可以使用现有数据库，例如，可使用默认情况下由 vCenter Server 附带的 Microsoft SQL Server 2005 Express 实例。

表 1-3 中列出了受支持的数据库类型及其要求。

表 1-3. View Composer 的数据库支持和要求

数据库类型	要求
Microsoft SQL Server 2000 Standard SP4	对于 Windows XP，在客户端中应用 MDAC 2.8 SP1。 客户端需使用 SQL Server 驱动程序。
Microsoft SQL Server 2000 Enterprise SP4	
Microsoft SQL Server 2005 Standard SP1 / SP2	对于 Windows XP，在客户端中应用 MDAC 2.8 SP1。 客户端需使用 SQL 本地客户端驱动程序。
Microsoft SQL Server 2005 Enterprise SP1 / SP2	
Microsoft SQL Server 2005 Express	
Microsoft SQL Server 2005 Standard Edition 64bit SP2	不适用
Microsoft SQL Server 2005 Enterprise Edition 64bit SP2	
Oracle 9i release 2 Standard (9.2.0.8)	
Oracle 9i release 2 Enterprise (9.2.0.8)	
Oracle 10g Standard Release 2 (10.2.0.1.0)	先在客户端和服务器中应用修补程序 10.2.0.3.0，然后在客户端中应用修补程序 5699495。
Oracle 10g Enterprise Release 2 (10.2.0.1.0)	
Oracle 10g Standard Release 1 (10.1.0.3.0)	不适用
Oracle 10g Enterprise Release 1 (10.1.0.3.0)	
Oracle 10g Enterprise Edition， Release 2 (10.2.0.1.0) 64 位	先在客户端中应用修补程序 10.2.0.3.0，然后再应用修补程序 5699495。
Oracle 10g Enterprise Edition， Release 2 (10.2.0.3.0) 64 位	不适用
Oracle 11g Standard Edition	与 VirtualCenter Server 2.5 不兼容。
Oracle 11g Enterprise Edition	与 VirtualCenter Server 2.5 不兼容。

安装 2

本章介绍如何安装和备份 View Connection Server 的一个或多个实例，并介绍在此操作过程中您可能遇到的不同部署方案。

在安装 View Connection Server 之前，请参阅第 11 页上的第 1 章，“简介”，以查看系统要求以及硬件和设备支持。

安装并配置 View Connection Server 之后，请参阅第 39 页上的 “备份 View Connection Server” 以获取有关如何备份 View Manager 配置信息的相关信息；有关如何配置 View 环境以支持大型桌面部署的相关信息，请参阅第 40 页上的 “优化您的安装操作”。

本章讲述以下主题：

View Connection Server 概述

View Connection Server 与 vCenter Server 进行通信，从而支持对虚拟桌面的高级管理。这包括作为池管理一部分的虚拟桌面创建，以及电源操作 （例如：自动挂起和恢复）。

View Connection Server 具备以下功能：

- 验证用户身份
- 通过 View LDAP 授予用户桌面权利
- 管理虚拟桌面会话
- 协调安全连接的建立、虚拟桌面的连接和单点登录
- 通过 View Administrator Web Client 管理服务器
- 管理虚拟桌面池

View Connection Server 实例

View Connection Server 安装在 Microsoft Windows Server 系统中，该系统位于专门用来充当 View Manager 连接中介器的物理服务器或虚拟服务器上。主机系统必须加入 Active Directory 域，但不能作为域控制器。您必须为主机系统指定静态 IP 地址。

警告 请勿在执行任何其他功能或角色的平台中安装 View Connection Server，例如，请勿使用同一系统安装 vCenter Server。

安装 View Connection Server 的域用户帐户必须对该服务器具有管理员权限。此外，View Connection Server 管理员还必须具有 vCenter Server 的管理凭据。

服务器既可作为标准服务器、副本服务器安装，也可以作为安全服务器安装。您可在安装过程中选择实例类型。

注释 要向非 View Connection Server （标准或副本）所在的 Active Directory 域中添加用户，必须在用户所在域和 View Connection Server 所在域之间建立双向信任关系。

配置域过滤器

View Manager 通过遍历信任关系确定可以访问哪些域，从 View Connection Server 实例或安全服务器所在的域开始。对于一组连接良好的小型域， View Manager 能够快速确定完整的域列表，但随着域数量的不断增多或域之间连通性能的逐渐降低，确定完整域列表所需的时间也会随之增加。另外，该列表中还可能包含您不希望在最终用户登录桌面时为其提供的域。

您可以使用 `vdmadmin` 命令来配置域的过滤，从而限制 View Connection Server 实例或安全服务器能够搜索到并向最终用户显示的域。有关详细信息，请参见《Command-Line Tool for View Manager》（View Manager 的命令行工具）技术说明。

View LDAP

View LDAP 是一种嵌入式轻型目录访问协议目录，它用于作为 View Manager 所有配置信息的数据存储库。 View LDAP 将作为 View Connection Server 安装的一部分提供。

View LDAP 包含 View Manager 中使用的以下组件：

- 特定的 View Manager 架构定义
- 目录信息树 (DIT) 定义
- 访问控制列表 (ACL)

View LDAP 包含表示以下 View Manager 对象的条目：

- 虚拟桌面条目，表示每个可访问的虚拟桌面，其中包含对 Active Directory 中有权使用此桌面的 Windows 用户和 Windows 用户组的外部安全规范 (FSP) 条目的引用
- 虚拟桌面池条目，表示被集中管理的多个虚拟桌面
- 虚拟机条目，表示每个虚拟桌面
- View Manager 组件配置条目，用于存储配置设置

此外， View LDAP 还包含一整套 View Manager 插件 DLL，可为其他 View Manager 组件提供自动化服务和通知服务。

注释 安全服务器实例不包含 View LDAP 组件。

安装标准服务器

部署标准服务器是指创建一台独立的 View Connection Server。稍后，此服务器可以成为可复制的 View Connection Server 组内的第一个服务器实例。

在 View Connection Server 安装过程中创建标准服务器实例时，系统还会创建新的本地 View LDAP 实例。架构定义、 DIT 定义和 ACL 等会被加载，且数据被初始化。

注释 尽管 View Connection Server 可自动管理一些条目，但 View LDAP 中的大多数配置数据仍由 View Administrator 维护。

安装标准服务器

1 在要安装 View Connection Server 的系统中运行以下可执行文件，其中 xxx 是指该文件的内部版本号：

```
VMware-viewconnectionserver-xxx.exe
```

随即显示 [VMware Installation（VMware 安装）] 向导。单击 **[Next（下一步）]**。

2 接受 VMware 许可条款并单击 **[Next （下一步）]**。

3 接受或更改目标文件夹，并单击 **[Next （下一步）]**。

4 选择 **[Standard （标准）]** 部署选项。

5 单击 **[Next （下一步）]** > **[Install （安装）]** > **[Finish （完成）]**。

安装副本服务器

副本服务器是指为了提供高可用性和负载平衡而安装的其他 View Connection Server 实例。安装副本服务器时，系统还将创建一个本地 LDAP 实例，且副本服务器中的 View LDAP 数据将利用现有的 View Connection Server 进行初始化。

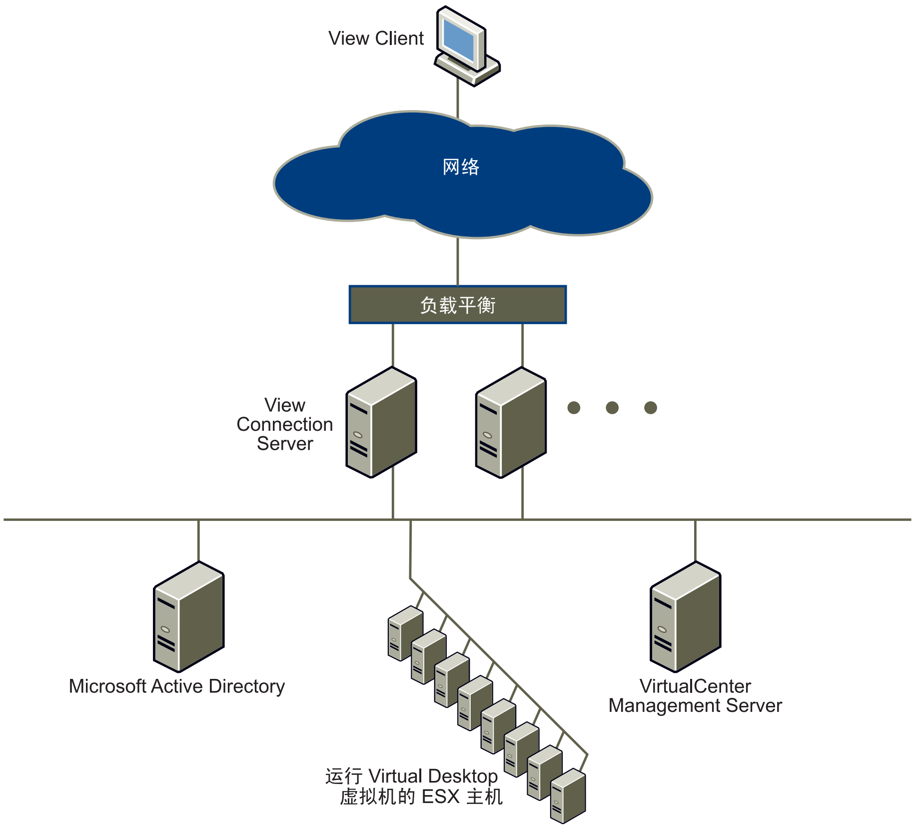
在安装副本服务器过程中将建立一份协议，确保已复制的组中每个 View Connection Server 均可共享相同的配置数据。无论何时，只要对一个系统中的 View LDAP 数据进行更改，则更改后的更新信息将自动传播至组内的所有其他副本服务器中。

注释 此复制功能由 LDAP 提供， LDAP 使用的复制技术与 Active Directory 相同。

要安装副本服务器，网络中必须至少已存在一个 View Connection Server 实例。副本服务器可以使用标准服务器或另一副本服务器来初始化其数据。进行初始化之后，副本服务器与标准服务器的行为和功能完全相同。

当服务器出现故障时，已复制的组中的其他服务器仍将继续正常运行。如果出现故障的服务器恢复活动，其配置数据将自动更新，以对故障期间发生的更改进行同步。图 2-1 显示了两个作为已复制的组运行的 View Connection Server 实例。

图 2-1. 多台副本服务器



要进一步增强 View 环境的高可用性和可扩展性，建议您部署负载平衡解决方案。这样可以确保所有连接负载均匀分布在每台可用的 View Connection Server 中，并且有故障的或不可访问的服务器将自动从已复制的组中排除。

注释 View Connection Server 不提供负载平衡功能，但支持标准的第三方负载平衡解决方案。

安装副本服务器

1 在要安装 View Connection Server 的系统中运行以下可执行文件，其中 xxx 是指该文件的内部版本号：

```
VMware-viewconnectionserver-xxx.exe
```

随即显示 [VMware Installation （VMware 安装）] 向导。单击 **[Next （下一步）]**。

2 接受 VMware 许可条款并单击 **[Next （下一步）]**。

3 接受或更改目标文件夹，并单击 **[Next （下一步）]**。

4 选择 **[Replica （副本）]** 部署选项。

5 输入要复制的现有 View Connection Server 的主机名或 IP 地址。如果目标系统与主服务器不属于相同域的组成部分，则必须具有目标服务器的本地管理权限才可执行此操作。

6 单击 **[Next （下一步）]** > **[Install （安装）]** > **[Finish （完成）]**。

安装安全服务器

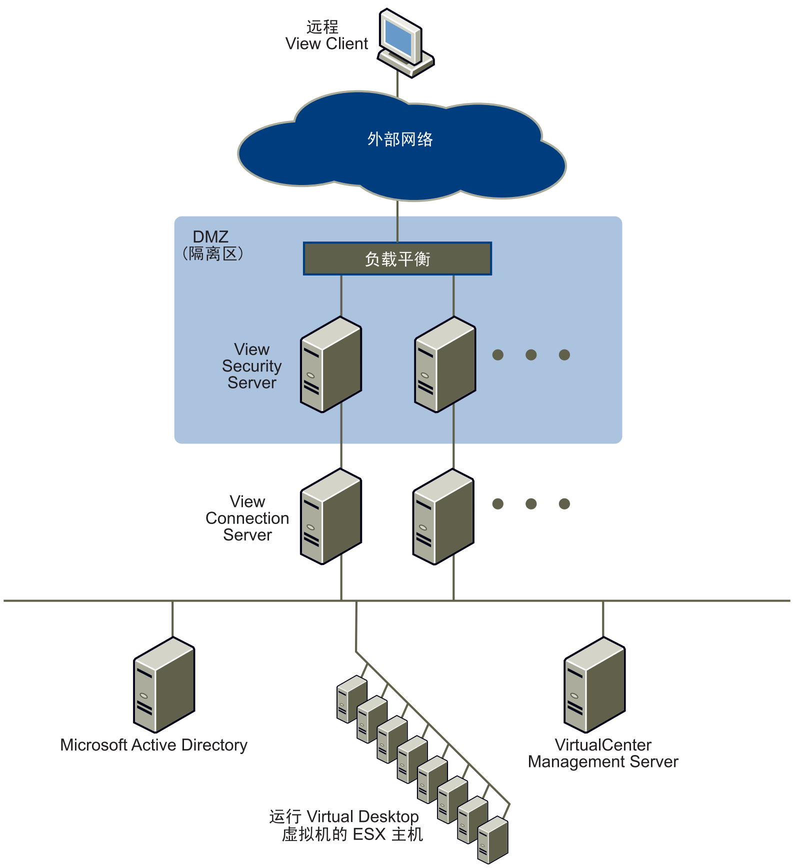
隔离区 (DMZ) 是指安全内部网络和不安全外部网络之间存在的部分受保护子网。此空间范围内的服务可供两个网络使用，并为访问安全环境内应用程序的外部用户提供入口点。

View Connection Server Security Server （安全服务器）安装在 DMZ 中，可增加一层网络保护，从而确保仅经过身份验证的用户才可通过提供单一访问点从外部位置连接到内部网络。由于 DMZ 服务的入站通信受到防火墙策略的严格控制，因此，内部网络泄露的风险将大幅度降低。

注释 在基于 LAN 的部署中，不要求使用安全服务器，因为用户可从其内部网络与任何 View Connection Server 直接相连。

图 2-2 显示了一个高可用性环境，该环境由位于 DMZ 中的两台负载平衡安全服务器组成，且这两台服务器与内部网络中的 View Connection Server 的两个实例 （即：标准服务器和副本服务器）进行通信。

图 2-2. 多台安全服务器



远程用户通过安全服务器进行连接时，他们必须成功通过身份验证后才可访问任何虚拟桌面。DMZ 的两端都有相关的防火墙规则，因此，此类部署特别适用于从位于 Internet 的客户端设备中访问虚拟桌面。

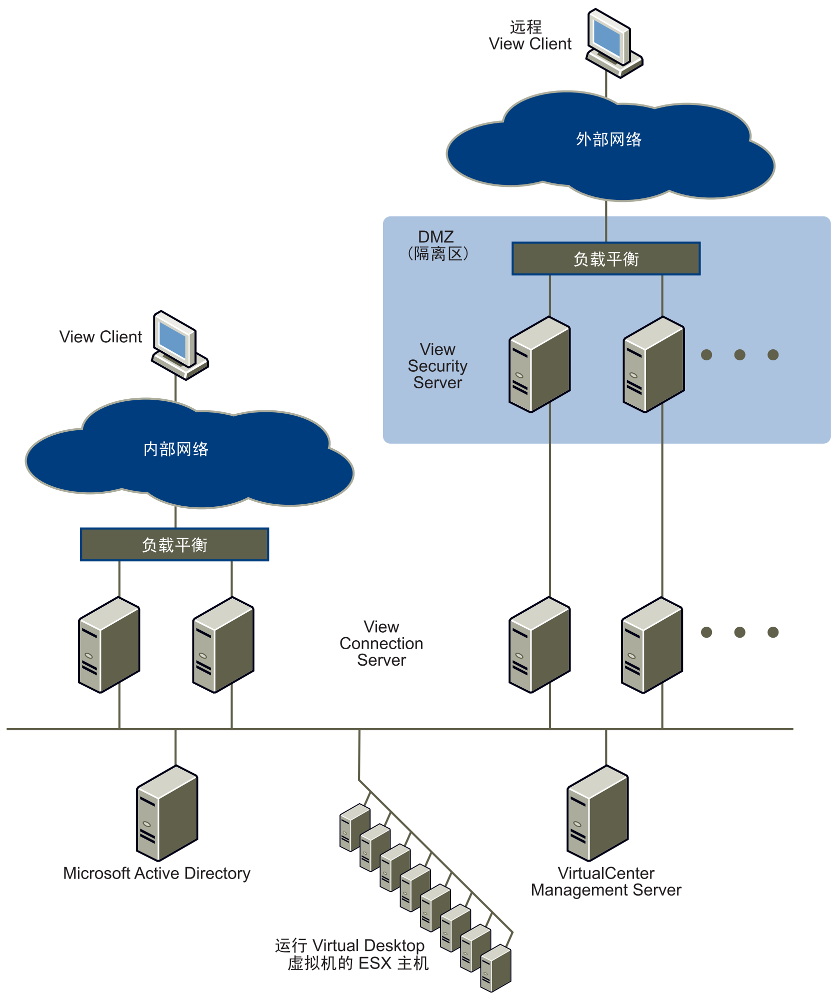
多台安全服务器可与每台标准或副本 View Connection Server 相连。DMZ 部署可与标准部署结合使用，以便支持内部用户和外部用户进行访问。

图 2-3 中， View Connection Server 的四个实例充当一个组，内部网络中的服务器专用于内部网络用户，而外部网络中的服务器则专用于外部网络用户。右侧的服务器可用于进行 RSA SecurID 身份验证，因此，所有外部网络用户都必须使用 RSA SecurID 令牌进行身份验证。

根据具体的服务器配置，可能会要求使用负载平衡。如果有一台以上安全服务器，则您将要求使用硬件或软件负载平衡解决方案。

注释 View Connection Server 不提供负载平衡功能，但支持标准的第三方负载平衡解决方案。

图 2-3. 含有多个 View Connection Server 实例的 DMZ 部署



安全服务器可实施部分 View Connection Server 功能，且无需驻留在 Active Directory 域中。此外，安全服务器还不包含 View LDAP 配置存储库，且不访问任何其他身份验证存储库，例如， Active Directory 或 RSA Authentication Manager。

安装安全服务器

1 请在要安装安全服务器的系统中运行以下可执行文件，其中 xxx 是指该文件的内部版本号：

```
VMware-viewconnectionserver-xxx.exe
```

随即显示 [Installation （安装）] 向导。单击 **[Next （下一步）]**。

2 接受许可条款并单击 **[Next （下一步）]**。

3 接受或更改目标文件夹，并单击 **[Next （下一步）]**。

4 选择 **[Security Server （安全服务器）]**。

5 每台安全服务器均与 View Connection Server 配对，并将所有流量转发给该服务器。输入安全服务器要通信的标准或副本服务器的 FQDN。

6 单击 **[Next （下一步）]** > **[Install （安装）]** > **[Finish （完成）]**。

External URL （外部 URL）

默认情况下， View Client 要求使用主机的 FQDN，以便与 View Connection Server 建立连接。尝试从网络环境外部联系服务器的客户端将无法获得该信息。

有关如何向安全服务器添加外部 URL、使其可从 Internet 访问的信息，请参阅第 93 页上的 “通过 Internet 执行客户端连接”。

Offline Desktop

如果打算使用 Offline Desktop 功能，则还必须确保同样可访问 ESX / ESXi 主机中的端口 902 ；此端口用来建立 TCP 连接，使用此连接，可下载和上传脱机桌面数据。有关此组件的详细信息，请参阅第 157 页上的第 7 章， “Offline Desktop”。

远程桌面 (RDP)

在桌面虚拟机或未被管理的桌面中安装 View Agent 时，该应用程序的安装程序将配置本地防火墙规则，使入站 RDP 连接与主机操作系统的当前 RDP 端口匹配。在大多数情况下，此端口应为 3389。

如果管理员随后更改 RDP 使用的端口号，则管理员必须同样修改桌面虚拟机或未被管理的桌面以及后端防火墙的相关防火墙规则。

有关桌面虚拟机和未被管理的桌面的详细信息，请参阅第 64 页上的 “桌面源”。

View Manager 用户的 vCenter Server 权限

要结合使用 vCenter Server 和 View Manager，管理员必须有权在 vSphere 中执行某些操作。通过从 vCenter Server 中创建角色并将其分配给 View Manager 用户，可以授予这些权限。

注释 vCenter Server 中的管理用户默认具有所有这些必备权限。

请为 View Manager 管理员分配要在其中创建池的数据中心或群集的管理员角色，使他们可以进行必需更改。

为 vCenter Server 用户创建 View Manager 角色

1 在 vSphere Client 中，单击 **[Administration （管理）]** > **[Roles （角色）]**。

2 单击 **[Add Role （添加角色）]** 以显示 [Add Role （添加角色）] 对话框。

3 为新角色输入唯一名称，如 `View Administrator`。

4 在 **[Privileges （权限）]** 列表中，展开 **[Folder （文件夹）]**，并依次选择 **[Create Folder （创建文件夹）]** 和 **[Delete Folder （删除文件夹）]**。

5 展开 **[Virtual Machine （虚拟机）]** 并执行以下步骤：

   a 展开 **[Inventory （清单）]**，依次选择 **[Create （创建）]** 和 **[Remove （删除）]**。

   b 展开 **[Interaction （交互）]**，依次单击 **[Power On （开机）]**、 **[Power Off （关机）]**、 **[Suspend （挂起）]** 和 **[Reset （重置）]**。

   c 展开 **[Configuration （配置）]**，依次选择 **[Add new disk （添加新磁盘）]**、 **[Add or Remove Device （添加或删除设备）]**、 **[Modify Device Settings （修改设备设置）]** 和 **[Advanced （高级）]**。

   d 展开 **[Provisioning （部署）]**，依次选择 **[Customize （自定义）]**、**[Deploy Template （部署模板）]** 和 **[Read Customization Specifications （读取自定义规范）]**。

6 展开 **[Resource （资源）]** 并选择 **[Assign Virtual Machine to Resource Pool （向资源池分配虚拟机）]**。

7 单击 **[OK （确定）]**。

角色列表中将显示新角色。

初始配置 View Manager

安装一个或多个 View Connection Server 实例之后，您必须执行初始配置，以便实例可准备执行管理任务。

您需从基于 Web 的 View Manager 管理组件 View Administrator 中执行此配置。第 47 页上的第 3 章，“View Administrator”中详细介绍了该组件。

注释 此组件仅在标准和副本服务器实例中可用。

执行初始配置

1 打开 View Administrator 支持的浏览器，输入以下 URL，其中 <server> 是指标准或副本 View Connection Server 实例的主机名或 IP 地址：

```
https://<server>/admin
```

注释 View Administrator 通过安全 (SSL) 连接进行访问。第一次连接时，浏览器可能会显示一页中间页面，警告您该地址相关的安全证书不是由可信的证书颁发机构颁发的。系统应当会显示此警告，因为 View Connection Server 附带提供的默认根证书是自签证书。

2 请使用适当的凭据登录。初始的配置中， View Connection Server 中的本地管理员组成员的所有域用户都可登录到 View Administrator，您稍后可在此界面中更改 View Manager 管理员列表。

第一次登录时，屏幕中将显示 [Configuration （配置）] 视图。获得产品许可证并登录后将显示 [Desktop （桌面）] 视图。

注释 如果未显示 [Configuration（配置）] 视图，单击屏幕上方的 **[Configuration （配置）]** （）按钮。

3 在 [Configuration （配置）] 视图中，执行以下操作：

a 在屏幕左侧的列中，单击 **[Product Licensing and Usage （产品许可和使用情况）]**。

b 在 [Product Licensing （产品许可）] 表中，单击 **[Edit License （编辑许可证）]**，并在弹出窗口的文本框中输入 View Manager 许可证密钥。单击 **[OK （确定）]**。

c 单击屏幕左侧列中的 **[Servers （服务器）]**。

d 在 **[vCenter Server]** 表中，单击 **[Add （添加）]**，并输入要与 View Manager 结合使用的一台或多台 vCenter Server 服务器的详细信息。

i 在 **[Server address （服务器地址）]** 文本框中，输入要与 View Manager 通信的 vCenter Server 的 FQDN 或 IP 地址。

警告 如果通过 DNS 名称或 URL 输入服务器，则系统将不执行任何 DNS 查找以验证先前是否曾使用 IP 地址输入该服务器。如果同时使用 DNS 名称和 IP 地址添加 vCenter Server，则会发生冲突。

ii 在 **[User name （用户名）]** 文本框中输入 vCenter Server 用户的用户名。如果要选择不是管理员、但具有必备权限级别的 vCenter Server 用户，确保其角色符合第 36 页上的 "View Manager 用户的 vCenter Server 权限" 中介绍的标准。

iii 在 **[Password （密码）]** 文本框中，输入与以上输入的用户名对应的密码。

iv （可选）在 **[Description （描述）]** 文本框中，输入此 vCenter Server 的描述。

v 如果要通过安全通道 (SSL) 连接到 vCenter Server，确保已选中 **[Connect using SSL （使用 SSL 连接）]**。这是默认设置。

vi 在 [Port （端口）] 文本框中，输入 TCP 端口号。默认端口号为 443。

vii （可选）如果单击 **[Advanced （高级）]** 按钮，还可配置以下设置：

viii **Maximum number of concurrent provisioning operations （并行部署操作的最大数）** – 这是指在任何给定时间内、 View Manager 可在 vCenter Server 中同时创建的虚拟机最大数。

ix **Maximum number of concurrent power operations （并行电源操作的最大数）** – 这是指在任何给定时间内、 View Manager 管理的虚拟机在 vCenter Server 中可能发生的并行电源操作 （开机、关机和挂起等）的最大数。

e 单击 **[OK （确定）]** 以存储 vCenter Server 设置。

f 单击屏幕左侧列中的 **[Administrators （管理员）]**。

g 在 [Administrators （管理员）] 表中，单击 **[Add （添加）]**，并使用提供的表单向需要访问 View Administrator 的 Active Directory 用户授予管理权限。添加所有必需的管理员之后，单击 **[OK （确定）]**。

备份 View Connection Server

要保留或迁移配置信息， View Manager 支持您在任何标准或副本 View Connection Server 中导入或导出 View LDAP 存储库内容。

View LDAP 数据以 LDAP 数据交换格式 (LDIF) 导出和导入，该格式是一种 Internet 文件格式试用标准，可用来对遵循 LDAP 标准的目录执行批处理操作。

对单个服务器或复制的组完成初始配置后，请定期备份 View Manager 数据。当数据协调一致时，一个实例丢失数据即意味着已复制的组中所有成员的相同数据均会丢失，因此，请勿依靠副本服务器作为备份机制。

要对 View LDAP 和 View Composer 数据计划常规自动备份，请使用 View Administrator 中提供的 View Manager 配置备份功能。第 55 页上的表 3-3，“View Server 设置”中介绍了该功能。

您还可以按照本部分中介绍的内容使用 `vdmexport.exe` 手动导出 View LDAP 数据。

注释 由于所有副本服务器均包含相同的配置数据，因此，如果已复制的组中存在多个 View Connection Server 实例，则您仅需从一台服务器导出数据。

可通过每个标准及副本 View Connection Server 附带的 `vdmexport.exe` 工具，从 View Manager 中导出 LDIF 数据。这个可执行文件的路径是：

```
C:\Program Files\VMware\VMware View\Server\bin\vdmexport.exe
```

导出 View Manager 配置数据

请以具有管理员权限的用户身份，通过标准或副本 View Connection Server 中的命令提示符执行以下命令：

```
vdmexport > vdmconfig.ldf
```

此命令可创建一个名为 `vdmconfig.ldf` 的文件，该文件包含已导出的 View LDAP 配置信息。

您可以使用 `LDIFDE` 将 LDIF 数据导入到 View Manager 中； LDIFDE 是 Windows Server 2003 附带的一款实用程序，它支持根据 LDIF 文件格式标准执行批处理操作。

导入 View Manager 配置数据

从标准或副本 View Connection Server 中的命令提示符中，更改到 LDAP 目录并执行以下命令：

```
cd C:\windows\adam
```

```
LDIFDE -i -f vdmconfig.ldf -s 127.0.0.1 -z
```

此命令可导入一个名为 `vdmconfig.ldf` 的文件，该文件包含之前已导出的 View LDAP 配置数据。

注释 `C:\Windows\System32` 中的默认 `LDIFDE` 不包含所需的 `-z` 参数。

优化您的安装操作

为支持大规模 View Manager 桌面部署，您可以对安装 View Connection Server 的 Windows Server 计算机进行优化。您可以在每个计算机中优化短周期端口、 TCB 哈希表大小、 Java 虚拟机设置和 Windows 页面文件大小。

有关 View Connection Server 的硬件和内存要求，请参见第 14 页上的 "系统要求"。

短周期端口

View Manager 使用短周期端口在 View Connection Server 与其管理的 View 桌面之间建立 TCP 连接。为支持大规模 View 桌面部署，您可以增加可用短周期端口的数量。

短周期端口是指当程序请求任何可用的用户端口时，由操作系统创建的短期使用的端口。操作系统会在预定义的范围内 （通常介于 1024 和 65535 之间）选择端口号，并在相关的 TCP 连接终止后释放这个端口。

默认情况下，您可以在 Windows Server 2003 中创建多达 4000 个同时运行的短周期端口。

如果您的 View Manager 部署要使用超过 800 个并发客户端连接，则应当增加可用短周期端口的数量。

要支持大量并发客户端连接，您可以计算在每个 View Connection Server 实例上配置的最理想的短周期端口数量。

计算短周期端口的数量

使用以下公式。

`短周期端口数量 = ((5 * 客户端数量 ) / 服务器数量 ) + 10`

其中

客户端数量 = 计划的并发客户端连接数

服务器数量 = 副本服务器组中 View Connection Server 实例的数量

例如，您可以规划一个由三个 View Connection Server 实例管理的部署。如表 2-1 中所示，如果您预计会有 3,000 个并发客户端连接，就需要设置 5,010 个短周期端口。

表 2-1. 示例：计算短周期端口的数量

配置参数	范例值
计划的并发客户端连接数	3,000
副本服务器组中 View Connection Server 实例的数量	3
((5 * 客户端数量) / 服务器数量) + 10 = 每个 View Connection Server 上的短周期端口数量	(5 * 3,000) / 3 + 10 = 5,010

使用第 44 页上的 "用于计算短周期端口和 TCB 哈希表的工作表" 填写相关的部署值。

您可以通过编辑 Windows 注册表来增加运行 View Connection Server 的 Windows Server 计算机上的短周期端口最大值。其前提是，必须计算要配置的短周期端口数量，如表 2-1 中所示。

增加短周期端口的数量

1 在 Windows Server 中，启动 Windows 注册表编辑器。

   a 选择 **[Start （开始）] > [Command Prompt （命令提示符）]**。

   b 通过命令提示符键入 `regedit`。

2 在注册表中找到正确的子项，然后单击 **[Parameters （参数）]**。

   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters`

3 单击 **[Edit （编辑）] > [New （新建）]**，添加注册表项。

```
Value Name：MaxUserPort
Value Type：DWORD
Value data：1024 +<计算出的短周期端口数量>
Valid Range：5000-65534 (decimal)
```

4 退出注册表编辑器。

5 重新启动 Windows Server 计算机。

Active Directory 组策略可重写注册表项。如果可能，请使用组策略来设置 View Connection Server 上的短周期端口数量。

增加 TCB 哈希表的大小

传输控制数据块 （Transmission Control Block， TCB）可保存与 View Connection Server 客户端及其桌面源之间的 TCP 连接有关的信息。要支持大规模 View 桌面部署，您可以增加 TCB 哈希表的大小。

TCB 是一种内存驻留数据结构，其中包含套接字编码、传入和传出数据缓冲的位置、已收到或未确认的字节以及其他信息。为了快速检索这些信息， Windows Server 将 TCB 数据结构存储在一个哈希表中。默认情况下，操作系统会根据 Windows Server 计算机的 CPU 数量配置哈希表的行数。

计算 View Connection Server 实例和安全服务器上的 TCB 哈希表大小时需要分别采用不同的公式。

为支持大量 View 桌面，您可以优化每个 View Connection Server 实例上的 TCB 哈希表大小。您可以以行为计算单位优化每个 View connection Server 实例上的 TCB 哈希表大小。

计算 View Connection Server 的 TCB 哈希表大小

使用以下公式。

```
每个 View Connection Server 实例上的哈希表行数 =
((5 * 客户端数量 ) / 服务器数量 ) + 桌面数量 + 20
```

其中

客户端数量 = 计划的并发客户端连接数

服务器数量 = 副本服务器组中 View Connection Server 实例的数量

桌面数量 = 部署中 View 桌面源的数量

例如，您的部署中可能会有 3,000 个并发客户端连接、三个 View Connection Server 实例和 6,000 个 View 桌面源。如表 2-2 中所示，每个 View Connection Server 实例对应的结果是 11,020。

表 2-2. 示例：计算 View Connection Server 上的 TCB 哈希表大小

配置参数	范例值
计划的并发客户端连接数	3,000
View Connection Server 实例的数量	3
View 桌面源的数量	6,000
((5 * 客户端数量) / 服务器数量) + 桌面数量 + 20 = 每台服务器的 TCB 哈希表行数	(5 * 3,000) / 3 + 6,000 + 20 = 11,020

使用第 44 页上的 “用于计算短周期端口和 TCB 哈希表的工作表”填写相关的部署值。

计算安全服务器的 TCB 哈希表大小

使用以下公式。

`哈希表行数 = ((5 * 客户端数量 ) / 安全服务器数量 ) + 10`

其中

客户端数量 = 计划的并发客户端连接数

安全服务器数量 = 安全服务器的数量

例如，您的部署中可能包含 3,000 个并发客户端连接。如表 2-3 中所示，每个安全服务器对应的结果是 7,510。

表 2-3. 示例：计算安全服务器上的 TCB 哈希表大小

配置参数	范例值
计划的并发客户端连接数	3,000
安全服务器数量	2
((5 * 客户端数量) / 安全服务器数量) + 10 = 每台安全服务器上的 TCB 哈希表行数	(5 * 3,000) / 2 + 10 = 7,510

使用第 44 页上的 "用于计算短周期端口和 TCB 哈希表的工作表" 填写相关的部署值。

在 Windows 注册表中设置 TCP 哈希表大小

您可以通过编辑 Windows 注册表来增加运行 View Connection Server 的 Windows Server 计算机上的 TCB 哈希表大小。

增大 Windows Server 上 TCB 哈希表的大小

1 在 Windows Server 中，启动 Windows 注册表编辑器。

   a 选择 **[Start （开始）] > [Command Prompt （命令提示符）]**。

   b 通过命令提示符键入 `regedit`。

2 在注册表中找到正确的子项，然后单击 **[Parameters （参数）]**。

   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters`

3 单击 **[Edit （编辑）] > [New （新建）]**，添加以下注册表项。

```
Value Name: MaxHashTableSize
Value Type: DWORD
Value data: <计算出的哈希表大小>
Valid Range: 64-65536 (decimal)
```

4 退出注册表编辑器。

5 重新启动 Windows Server 计算机。

Active Directory 组策略可重写注册表项。如果可能，请使用组策略来设置 View Connection Server 中的 TCB 哈希表大小。

用于计算短周期端口和 TCB 哈希表的工作表

使用此工作表可计算部署中每个 View Connection Server 和安全服务器上的短周期端口数量与 TCB 哈希表大小。

表 2-4. 用于计算短周期端口数量和 TCB 哈希表大小的工作表

配置参数	**填入对应值**
计划的并发客户端连接数	
View Connection Server 实例的数量	
安全服务器数量	
View 桌面源的数量	
短周期端口数量	**填入对应值**
((5 * 客户端数量) / 服务器数量) + 10 = 每个 View Connection Server 上的短周期端口数量	
View Connection Server 的 TCB 哈希表大小	**填入对应值**
((5 * 客户端数量) / 服务器数量) + 桌面数量 + 20 = 每台服务器的 TCB 哈希表行数	
安全服务器的 TCB 哈希表大小	**填入对应值**
((5 * 客户端数量) / 安全服务器数量) + 10 = 每台安全服务器上的 TCB 哈希表行数	

优化 Java 虚拟机

您可以增加 Java 虚拟机 (Java Virtual Machine， JVM) 堆内存配置的大小，以支持大量并发 View 桌面会话。View Connection Server 使用自己的 JVM 实例运行其应用程序进程。

View Connection Server JVM 默认的堆大小为 512 MB。此配置可支持约 750 个并发 View 桌面会话。

JVM 堆内存是以连续内存块的形式实施的。在 32 位 Windows 计算机上，分配的连续内存块的最大大小为 2 GB。 JVM 需要该空间的 0.5 GB 用于支持正常运行。因此，在 32 位 Windows 计算机上， JVM 程序最多只能使用约 1.5 GB 的内存来运行每个进程。

您可以通过编辑 Windows 注册表来增加安装 View Connection Server 的 Windows Server 计算机上 JVM 堆的大小。配置 1 GB 的 JVM 堆大小后，View Connection Server 就能支持约 1,500 个并发 View 桌面会话。

警告 切勿分配大小超过 1.5GB 的 JVM 堆。这样会导致 View Connection Server 服务无法启动。

您必须在每次安装或升级 View Connection Server 软件时增加 JVM 堆的大小。

增加 Windows Server 计算机上的 JVM 堆大小

1 在 Windows Server 计算机中，启动 Windows 注册表编辑器。

   a 选择 **[Start （开始）] > [Command Prompt （命令提示符）]**。

   b 通过命令提示符键入 `regedit`。

2 在注册表中找到正确的子项，然后单击 **[JvmOptions]**。

```
HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Plugins\
    wsnm\tunnelService\Params
```

3 单击 **[Edit （编辑）] > [Modify （修改）]**。

   Windows 对话框将显示与以下示例类似的注册表项：

```
-Xms128m -Xmx512m -Dsimple.http.poller=simple.http.GranularPoller
-Dsimple.http.connect.configurator=com.vmware.vdi.front.SimpleConfigurator
```

4 编辑 `-Xmx` 参数，将其值改为 **`-Xmx1024m`**。

   对话框将显示以下注册表项：

```
-Xms128m -Xmx1024m -Dsimple.http.poller=simple.http.GranularPoller
-Dsimple.http.connect.configurator=com.vmware.vdi.front.SimpleConfigurator
```

5 单击 **[OK （确定）]**，然后退出注册表编辑器。

6 重新启动 Windows Server 计算机。

配置系统页面文件设置

通过更改系统页面文件设置，您可以为安装了 View Connection Server 实例的 Windows Server 计算机优化虚拟内存。

安装 Windows Server 后，操作系统会根据计算机的物理内存计算页面文件的初始大小和最大大小。重新启动计算机后，这些默认值设置将保持不变。

如果 Windows Server 计算机是一个虚拟机，您可以通过 vCenter Server 来修改内存大小。然后，只要 Windows 采用了默认设置，系统的页面文件大小就不会调整为新的内存大小。

配置系统页面文件设置

1 在安装了 View Connection Server 的 Windows Server 计算机上，导航至 [Virtual Memory （虚拟内存）] 对话框。

   默认情况下， **[Custom size （自定义大小）]** 选项会被选中，并会显示页面文件大小的初始大小和最大大小。

2 单击 **[System managed size （系统管理的大小）]**。

Windows 会根据当前的内存使用情况和可用内存空间，不断重新计算系统页面文件的大小。

View Administrator 3

在 View Administrator 中，可以执行与 View Manager 和桌面管理相关的所有配置、部署、分析及管理任务。

本章讲述 View Administrator 的功能及您可以执行的任务。

本章讲述以下主题：

View Administrator 概述

在管理界面的顶部，显示 **[Desktops and Pools （桌面和池）]** （ ）、 **[Users and Groups （用户和用户组）]** （ ）、 **[Configuration （配置）]** （ ）和 **[Events （事件）]** （ ）按钮。使用这些按钮，您可导航至不同的功能区执行各种任务。

以下各节介绍了每个按钮的相关视图及功能。

桌面和池的视图

在您登录到 View Administrator 或单击 **[Desktops and Pools （桌面和池）]** 按钮时，默认情况下会显示 [Desktops and Pools （桌面和池）] 视图，您可以在此视图中创建、部署、管理和监视虚拟桌面。

在此视图中，您可以检查桌面或桌面池及其关联用户的信息、单个桌面源、任何处于活动状态的会话、任何已计划的任务，以及全局级别、池级别或用户级别的桌面使用策略。

[Desktops and Pools （桌面和池）] 视图可分为左侧和右侧窗格两个部分。左侧窗格包含 **[Inventory （清单）]** 和 **[Search （搜索）]** 选项卡；右侧窗格显示当前可用桌面的全局信息或池级信息。

选中 **[Inventory （清单）]** 选项卡后，将在左侧窗格中的 **[Global desktop and pool view （全局桌面和池视图）]** 顶层条目 () 下面，按字母顺序列出所有桌面或池。该条目的范围是全局的。选中该条目，可以更改右侧窗格的内容，使其包含所有可用桌面。

例如，选中该条目后，右侧窗格中的 **[Active Sessions （活动会话）]** 选项卡将列出所有 View Manager 桌面的所有活动会话。

如果提供了任何桌面或桌面池，将在 **[Global desktop and pool view （全局桌面和池视图）]** 条目下面列出它们。选中单个桌面 () 或桌面池条目 () 可更改右侧窗格的内容，提供该桌面或池的特定信息。

例如，如果选中此列表中的某一条目，则右侧窗格中的 **[Active Sessions （活动会话）]** 子选项卡将为该池中的桌面列出所有活动会话。

表 3-1 中描述了右侧窗格中的选项卡。此表 "内容" 列中的条目可指示所显示的选项卡：

- Desktop （桌面） – 选中单个桌面 () 时，显示此选项卡。
- Desktop Pool （桌面池） – 选中桌面池条目 () 时，显示此选项卡。
- Global （全局） – 选中 **[Global desktop and pool view （全局桌面和池视图）]** 条目 () 时，显示此选项卡。
- All （所有） – 以上内容中均会显示此选项卡。

表 3-1. 桌面窗格的选项卡摘要

选项卡	内容	描述
Summary **（摘要）**	Desktop （桌面） Desktop Pool （桌面池）	此选项卡显示桌面或桌面池所有相关信息的概述，包括： 桌面池的常规信息，例如：名称、类型、持久性和当前活动。 vCenter Server 环境标准，例如：服务器名、容量和域管理员。 桌面设置，例如：最大桌面数、最小桌面数、可用桌面数、电源策略等。 在这个选项卡中，您可以单击： ■ **[Edit （编辑）]**，以修改桌面或桌面池的部署设置。您可在该向导的左侧导航窗格中选择要修改其设置的页面。如果所做更改要求您修改其他页面的设置，则在导航窗格中，这些页面的旁边将出现信息图标。 ■ **[Entitle （授权）]**，以便在桌面或桌面池中添加或删除用户授权。 ■ **[Enable/Disable （启用 / 禁用）]**，以便启用或禁用桌面或桌面池的可用性和部署。
Desktops **（桌面）**	Global （全局）	此选项卡列出 View Manager 内当前可用的所有桌面或桌面池。在这个选项卡中，您可以单击 **[Add （添加）]** 以部署新的桌面或桌面池。 此外，您还可从显示的表中选择现有的桌面或桌面池条目，然后单击： ■ **[Edit （编辑）]**，以修改桌面或桌面池的部署设置。您可在该向导的左侧导航窗格中选择要修改其设置的页面。如果所做更改要求您修改其他页面的设置，则在导航窗格中，这些页面的旁边将出现信息图标。 ■ **[Entitle （授权）]**，以便在桌面或桌面池中添加或删除用户授权。 ■ **[Delete （删除）]**，以删除桌面或桌面池。 ■ **[Enable/Disable （启用 / 禁用）]**，以便启用或禁用桌面或桌面池的可用性和部署。
Users and Groups **（用户和用户组）**	Desktop （桌面） Desktop Pool （桌面池）	此选项卡列出有权使用此桌面或桌面池的所有用户和用户组。从 **[Entitlements （授权）]** 子选项卡下面，您可以从显示的表中列出的任何用户中选择并 **[Remove Entitlement （删除授权）]**。 如果选定的池使用链接克隆技术进行部署，则还会显示另一个子选项卡：**[Users and Groups （用户和用户组）]**。

表 3-1. 桌面窗格的选项卡摘要 （续）

选项卡	内容	描述
Desktop Sources （桌面源）	Desktop （桌面） Desktop Pool （桌面池）	此选项卡列出所选池中可用的所有单个虚拟系统。使用此选项卡，您可从显示的表中选择现有的桌面或桌面池条目，然后单击： ■ **[Remove （删除）]**，以便从 View Manager 或者 vCenter Server 和 View Manager 中删除单个或多个虚拟机 ■ **[Reset （重置）]**，以便重置所选桌面，此操作将中断目前已连接的任何用户，并重新启动系统 ■ **[Rebalance （重新平衡）]**，以便重新分发数据存储中的虚拟机，从而确保各个逻辑驱动器 （仅指 View Composer 桌面）中采用最佳方式使用空间 ■ **[Cancel Task （取消任务）]**，以便终止针对所选虚拟机 （仅指 View Composer 桌面）的已计划任务，或当前正在运行的任务
Active Sessions （活动会话）	All （所有）	此选项卡会列出全局范围内或所选池内当前处于活动状态的所有桌面会话。此外，还将显示已连接的每个用户的用户名、开始时间、持续时间和虚拟机地址。 您可以从显示的表中选择用户条目，然后单击： ■ **[Disconnect session （断开会话）]**，以断开用户与桌面的连接；但此操作不会注销用户，且如果桌面部署过程中所指定的 **[Automatic logoff after disconnect （断开后自动注销）]** 设置尚未超过限制，此操作将保留其会话，直到用户重新登录 ■ **[Logoff session （注销会话）]**，以便注销用户并将其与当前会话断开连接 ■ **[Reset virtual machine （重置虚拟机）]**，以断开目前已连接的用户并重新启动系统
Offline Sessions （脱机会话）	All （所有）	此选项卡会列出全局范围内或所选池内当前已检出的所有 Offline Desktop 桌面。 有关此功能及该选项卡提供的各种功能的更多信息，请参阅第 157 页上的第 7 章，"Offline Desktop"。
Global Policies （全局策略）	Global （全局）	此选项卡将列出应用到全局级别中所有桌面和池的策略。

表 3-1. 桌面窗格的选项卡摘要 （续）

选项卡	内容	描述
Tasks （任务）	Desktop Pool （桌面池）	该选项卡包含通过池进行的任何部署或维护任务的详细信息。 此视图提供有关计划任务开始时间、任务进程中可能已经遇到的任何错误及任务是否已暂停等方面的信息。 如果一个或多个任务正在进行中，您可以从显示的表中选择各个条目，然后单击： ■ **[Cancel Task （取消任务）]**，以终止任务 ■ **[Pause Task （暂停任务）]**，以暂停任务 ■ **[Resume Task （恢复任务）]**，以恢复任务：如果之前已经暂停任务 （由 [Halted （停止）] 列指示），选择该条目可恢复任务
Policies **（策略）**	Desktop （桌面） Desktop Pool （桌面池）	此选项卡可列出应用到所选桌面或桌面池的策略。该视图中也会列出已应用的任何用户级策略。

用户和用户组视图

单击 **[Users and Groups （用户和用户组）]** 按钮可显示 [Users and Groups （用户和用户组）] 视图；在此视图中，可监视桌面分配情况和已授权的 View Manager 用户的活动会话。

在此视图中，您可以检查用户及关联用户组的信息、查看分配给这些用户的桌面及他们的活动会话，以及在全局级别评估用户授权。

注释 对比 [Desktops and Pools （桌面和池）] 视图，该视图提供的功能较少；但是，您可从中针对每个用户断开或注销活动会话、重置虚拟机，以及回滚脱机桌面 （如果可用）。

[Users and Groups（用户和用户组）] 视图可分为左侧和右侧窗格两个部分。左侧窗格包含 **[Inventory （清单）]** 和 **[Search （搜索）]** 选项卡；右侧窗格显示当前授权的用户的全局信息或池级信息。

选中 **[Inventory （清单）]** 选项卡后，将在左侧窗格中的 **[Global users and group view （全局用户和用户组视图）]** 顶层条目下面，按字母顺序列出所有用户。该条目的范围是全局的。选中该条目，可以更改右侧窗格的内容，使其包含所有可用的用户。

例如，选中该条目后，右侧窗格中的 **[Active Sessions （活动会话）]** 选项卡将列出所有 View Manager 用户的所有活动会话。

如果用户或用户组存在，将在 **[Global users and group view （全局用户和用户组视图）]** 条目下面列出它们。选中单个用户或用户组条目可更改右侧窗格的内容，提供该用户或用户组的特定信息。

例如，如果选中此列表中的某一条目，则右侧窗格中的 **[Active Sessions （活动会话）]** 子选项卡将列出该用户或用户组中任何用户的所有活动会话。

表 3-2 中描述了右侧窗格中的选项卡。此表 “内容” 列中的条目可指示所显示的选项卡：

- User （用户） – 选中单个用户时，显示此选项卡。
- User Group （用户组） – 选中桌面池条目时，显示此选项卡。
- Global （全局） – 选中 **[Global users and group view （全局用户和用户组视图）]** 条目时，显示此选项卡。
- All （所有） – 以上内容中均会显示此选项卡。

表 3-2. 用户窗格的选项卡摘要

选项卡	内容	描述
Summary （摘要）	User （用户） Group （用户组）	此选项卡显示与选定的用户或用户组相关的所有信息，包括诸如以下内容的一般信息： ■ 用户数 （仅针对用户组） ■ 子组数 （仅针对用户组） ■ 默认域 ■ 联络详细信息 （如果可用，仅针对用户） ■ 活动会话 （仅针对用户） ■ 组成员 （仅针对用户） ■ 桌面和桌面池授权
Entitled Users and Groups （已授权的用户和用户组）	Global （全局）	此选项卡可完整列出获得授权以使用 View Connection Server 所管理的桌面和桌面池的所有用户及用户组。 同时，还提供每个用户的默认域、每个用户获准使用的桌面或池的数量，以及所有活动会话。
Desktops and Pools （桌面和池）	User （用户） Group （用户组）	此选项卡显示特定用户或用户组的桌面授权信息。 其显示的信息与 **[Entitled Users and Groups （已授权的用户和用户组）]** 选项卡相同，并说明所选用户或用户组获准使用的桌面或池的类型。

表 3-2. 用户窗格的选项卡摘要 （续）

选项卡	内容	描述
Active Sessions （活动会话）	All （所有）	此选项卡列出当前活动的所有桌面会话，既包含全局会话，又包含所选用户或用户组的会话。此外，还将显示已连接的每个用户的用户名、开始时间、持续时间和虚拟机地址。 您可以从显示的表中选择用户，然后单击： ■ **[Disconnect session （断开会话）]**，以断开用户与桌面的连接；但此操作不会注销用户或用户组，且如果桌面部署过程中所指定的 **[Automatic logoff after disconnect （断开后自动注销）]** 设置尚未超过限制，此操作将保留其会话，直到用户重新登录 ■ **[Logoff session （注销会话）]**，以便注销用户并将其与当前会话断开连接 ■ **[Reset virtual machine （重置虚拟机）]**，以断开目前已连接的用户并重新启动系统
Offline Sessions （脱机会话）	All （所有）	此选项卡会列出全局范围内或选定用户当前已检出的所有 Offline Desktop 桌面。 有关此功能及该选项卡提供的各种功能的更多信息，请参阅第 157 页上的第 7 章，“Offline Desktop”。

配置视图

单击 **[Configuration （配置）]** 按钮时，系统将显示 [Configuration （配置）] 视图。此视图包含多个部分，允许您分析桌面使用情况，配置许可证、连接和身份验证标准，等等。屏幕左侧的窗格中会列出每个部分。单击列表中的任一条目，便可显示与该部分相关的配置信息。

产品许可和使用情况

[Product Licensing（产品许可）] 表指出 View Manager 的许可证状态，并指出在该许可证范围内是否提供其他组件，例如 View Composer、 Offline Desktop 功能。

单击 **[Edit License（编辑许可证）]** 可添加或修改 View Connection Server 的许可证序列号。

[Usage （使用情况）] 表指出当前活动桌面的使用信息，其中包括 View Manager 许可证范围涵盖 Offline Desktop 时脱机桌面的使用信息。

- 单击 **[Refresh （刷新）]** 可更新 [Usage （使用情况）] 表中显示的信息。
- 单击 **[Reset highest （重置最大数）]**，可以重置用来计算并发连接最大数的计数器。

服务器

该部分中的各表介绍 View Connection Server 与出现在您的环境中的所有其他副本服务器及安全服务器之间的关系。并且，还提供 View Connection Server 用于管理其虚拟机的 vCenter Server 的相关信息。

vCenter Server 与安全服务器之间的关系是手动建立的，您可以使用每个表在列表中添加或删除服务器。在副本服务器组中， View 服务器之间的关系是在安装过程中定义的，可以自动检测到。

vCenter Server

vCenter Servers 表列出了可供 View Connection Server 使用的 vCenter Server 服务器。单击 **[Add （添加）]**、 **[Edit （编辑）]** 或 **[Remove （删除）]** 可修改连接标准。

第 37 页上的 "初始配置 View Manager" 中介绍了将服务器添加到此表的过程。

安全服务器

安全服务器在 DMZ 内工作，并运行 View Connection Server 完整功能的一部分。通过将安全服务器用作中间连接层， View Manager 可以确保只有经过身份验证的用户才能尝试连接到内部网络。

安全服务器进一步增强了这些环境 （允许客户端通过 Internet 访问它们）的网络安全性。有关此操作的详细信息，请参阅第 32 页上的 "安装安全服务器"。

[Security Servers （安全服务器）] 表可让您将一个或多个安全服务器实例添加到 View Manager 环境中。使用所提供的链接，您可以执行 **[Add （添加）]**、 **[Edit （编辑）]** 或 **[Remove （删除）]** 操作来添加、编辑或删除您的环境中的安全服务器的相关信息。

[Create Configuration File （创建配置文件）] 链接用于加快配置文件的创建过程，允许安全服务器准确地传输从 Internet 接收的客户端请求。有关外部连接的详细信息，请参阅第 93 页上的 "通过 Internet 执行客户端连接"；有关该功能的详细信息，请参阅第 95 页上的 "从 [Configuration （配置）] 视图中生成安全服务器的 config.properties 文件"。

View Server

在 [View Servers] 表中，您可以启用或禁用当前的 View Connection Server（以复选标记指示），以及该服务器已知的任何 View Connection Server 副本实例。从显示的表中选择一个服务器条目，并单击：

- **[Enable （启用）]**，允许用户使用该服务器连接到客户端。
- **[Disable （禁用）]**，拒绝客户端以后连接到该服务器。现有客户端连接不受此操作的影响。
- **[Edit （编辑）]**，显示 [View Server Settings （View Server 设置）] 窗口，您可以在此窗口中修改各种通信及身份验证属性。表 3-3 中描述了这些属性。
- **[Backup Now （立即备份）]**，立即对所有 View Connection Server 启动服务器备份。

注释 [View Server Settings （View Server 设置）] 窗口中的 [View Manager Configuration Backup （View Manager 配置备份）] 属性组，允许您针对 View Connection Server 数据来配置自动备份计划。请参阅第 55 页上的表 3-3，“View Server 设置”。

有关如何导入 View LDAP 数据和 View Composer 数据的信息，请参阅第 39 页上的 “备份 View Connection Server” 和第 155 页上的 “还原 View Composer 数据库 （restoredata）”。

表 3-3. View Server 设置

属性	描述
External URL **（外部 URL）**	要让外部客户端能够与 View Connection Server 进行通信，您必须输入一个能够外部解析的 URL。 在 **[External URL （外部 URL）]** 字段中输入 URL。该名称必须包含协议、地址和端口号。例如： `https://view.example.com:443` 有关该属性的详细信息，请参阅第 93 页上的 “通过 Internet 执行客户端连接”。
Direct connection to desktop **（直接连接到桌面）**	如果您希望由 View Connection Server 服务器代理的客户端连接使用直接 （非安全加密链路）连接，请选中此复选框。

表 3-3. View Server 设置 （续）

属性	描述
Smart card authentication （智能卡身份验证）	与此属性相关的下拉菜单提供了以下选项： ■ **[Not allowed （不允许）]**：表示已禁用智能卡身份验证。 ■ **[Optional （可选）]**：表示用户可以使用智能卡身份验证进行连接，但亦允许使用密码身份验证。 如果无法使用智能卡身份验证进行身份验证，则需要使用密码身份验证。 ■ **[Required （必需）]**：表示用户仅可使用智能卡身份验证进行连接。 配置智能卡移除策略 （如允许）： ■ 如果希望在用户移除智能卡时与 View Connection Server 实例断开连接，请选中 **[Disconnect user sessions on smart card removal （移除智能卡时断开用户会话）]** 复选框。用户必须重新进行身份验证，才能访问其 View 桌面。 ■ 取消选择该复选框，允许用户在移除智能卡时保持与 View Connection Server 实例的连接。用户无需重新进行身份验证即可发起新的 View 桌面会话。 智能卡移除策略不适用于在选择了 **[Log on as current user （作为当前用户登录）]** 复选框的情况下连接 View Connection Server 实例的用户，即使他们使用智能卡来登录其客户端系统，也无法使用此策略。 必须重新启动 View Connection Server 服务，对智能卡设置所做的更改才能生效。智能卡设置的变化不会对当前登录的用户造成影响。 有关智能卡身份验证功能的更多信息，请参阅第 101 页上的 "智能卡身份验证"。

表 3-3. View Server 设置 （续）

属性	描述
RSA SecurID 2-Factor Authentication （RSA SecurID 双因素身份验证）	该组中的各个属性可确定客户端在连接 View Connection Server 时是否还须使用 RSA SecureID 进行身份验证： ■ **[Enable （启用）]** – 确定客户端身份验证进程是否需要 RSA SecureID 凭据。 ■ **[Enforce SecurID and Windows user name matching （强制 SecurID 和 Windows 用户名相匹配）]** – 确定 RSA SecurID 用户名是否必须与存储在 Active Directory 中的用户名相匹配。 ■ **[Clear node secret （清除节点秘密）]** – 清除 View Agent 中的节点秘密。 ■ **[Upload RSA authentication agent configuration file (sdconf.rec) （上传 RSA 身份验证代理配置文件 （sdconf.rec））]** – 单击 [Browse （浏览）] 按钮，可选择并上传从该服务器的 RSA Authentication Manager 导出的 sdconf.rec 文件。 有关该功能的详细信息，请参阅第 109 页上的 "RSA SecurID 身份验证" 及 RSA 在 http://www.rsa.com/rsasecured 网站上为合作伙伴提供的支持文档。

表 3-3. View Server 设置 （续）

属性	描述
View Manager Configuration Backup （View Manager 配置备份）	为保留您的配置信息，View Manager 允许您备份您的环境中的所有 View Connection Server 使用的 View LDAP 存储库内容。 该属性组中的各个属性可确定 View Connection Server 自动备份（包括 View Composer 数据库数据）的计划标准。 ■ **[Automatic backup frequency （自动备份频率）]**：从以下各项中选择一个备份时间间隔： 　■ **[Every Hour （每小时）]**：每小时整点进行一次备份 　■ **[Every 6 Hours （每 6 个小时）]**：每天零点、上午 6 点、中午 12 点、下午 6 点进行备份 　■ **[Every 12 Hours （每 12 个小时）]**：每天零点和中午 12 点进行备份。 　■ **[Every Day （每天）]**：每天零点进行备份 　■ **[Every 2 Days （每 2 天）]**：星期六、星期一、星期三和星期五的零点进行备份 　■ **[Every Week （每周）]**：每周星期六的零点进行备份 　■ **[Every 2 Week （每 2 周）]**：每隔一周的星期六的零点进行备份 　■ **[Never （从不）]**：从不进行备份，必须手动进行备份 ■ **[Max number of backups （最大备份数）]**：指出在任意给定时间可存储在 View Connection Server 上的早期备份文件的数量。 当达到这一级别后，每当创建一个新的备份文件时，会同时删除备份文件夹中最早的备份文件。此数字必须是大于 `0` 的整数。 此设置同样适用于使用 View Server 表中的 **[Backup Now （立即备份）]** 链接手动创建的备份文件。 ■ **[Folder Location （文件夹位置）]**：备份文件的所在位置。默认位置： `C:\Documents and Settings\All Users\Application Data\VMware\VDM\backups` 此位置同样可以存储使用 View Server 表中的 **[Backup Now （立即备份）]** 链接手动创建的备份文件。

Registered Desktop Sources （已注册的桌面源）

此部分提供当前在 View Connection Server 中注册的终端服务源及其他源 （独立虚拟机以及物理桌面源）的数量。

Administrators （管理员）

[Administrators （管理员）] 表包含了可以登录到 View Administrator 的所有用户及用户组的列表。此列表中的所有条目都驻留在当前 Active Directory 域林中。

- 单击 **[Add（添加）]** 可以搜索 Active Directory 用户或用户组，以便将它们添加为 View Connection Server 管理员。

  a 此时会显示 [Add Administrator （添加管理员）] 窗口。从该窗口中，您可以查看、搜索和过滤该域林内的所有 Active Directory 用户。

  b 在 **[Type （类型）]** 中，选中 **[Users （用户）]** 复选框和 / 或 **[Groups （用户组）]** 复选框。

  c 从 **[Domain （域）]** 下拉菜单中，选择包含要添加的用户或用户组的域，或选择 **[Entire Directory （完整目录）]** 以搜索整个 Active Directory 域林。

  d 使用显示的字段，您可以按名称或描述进行搜索。单击 **[Find （查找）]** 执行搜索。

  注释 如果要查看域中的所有用户列表，请将 **[Name （名称）]** 和 **[Description （描述）]** 字段保留为空。

  e 从此表中，选择要添加的用户或用户组，然后单击 **[OK （确定）]**。

- 要从列表中删除管理员，请选择其对应的条目并单击 **[Remove （删除）]**。

Global Settings （全局设置）

此部分提供应用于该产品所有方面的全局产品配置参数的信息。要更改设置，请单击 **[Edit （编辑）]**，然后修改表 3-4 中的任一条目。

表 3-4. Global Settings （全局设置）

属性	描述
Session timeout （会话超时）	确定用户登录到 View Connection Server 之后，在多长时间（以分钟为单位）之内允许其会话保持打开。此字段必须包含一个值，默认值为 `600`。
Use SSL for client connections （使用 SSL 进行客户端连接）	确定是否使用 SSL 在 View Connection Server 与客户端之间创建安全通信通道。 如果您要使用智能卡身份验证，则必须启用该设置。
Reauthenticate Secure VPN connections after network interruption （网络中断后对安全的 VPN 连接重新进行身份验证）	确定在网络中断后是否必须对安全加密链路客户端用户凭据重新进行身份验证。使用直接连接时，此设置无效。
Message security mode （消息安全模式）	确定是否对 View Manager 3.x 和 4.x 组件之间传输的 JMS 消息进行了签发和验证。如果 View 环境中的任何组件早于 View Manager 3.0 版，则无法进行签发和验证。 ■ **[Disabled （禁用）]**：禁用消息安全模式。 ■ **[Mixed （混合）]**：启用消息安全模式，但并非强制使用。此模式可用于检测系统环境中早于 View Manager 3.0 版的组件，因为 View Connection Server 生成的日志文件将包含对这些组件的引用。 ■ **[Enabled （启用）]**：完全启用消息安全模式。早于 View Manager 3.0 版的组件在尝试通信时将被拒绝。 如果 View Manager 环境中有一台安全服务器，且您已启用此设置，则安全服务器中必须有一个经过正确配置的 `config.properties` 文件。 有关此操作的详细信息，请参阅第 95 页上的 "从 [Configuration （配置）] 视图中生成安全服务器的 config.properties 文件"。 View Manager 3.1 和更高版本支持消息安全模式。如果将消息安全模式由 **[Disabled （禁用）]** 或 **[Mixed （混合）]** 更改为 **[Enabled （启用）]**，您将无法通过 Virtual Desktop Manager 2.1 或更早版本启动 View Agent 的桌面。如果您将消息安全模式从 **[Enabled （启用）]** 更改为 **[Mixed （混合）]** 或 **[Disabled （禁用）]** 后桌面仍无法启动，那么，要在将消息安全模式从 **[Enabled （启用）]** 更改为 **[Mixed （混合）]** 或 **[Disabled （禁用）]** 后启动桌面，必须重新启动受影响的桌面。

表 3-4. Global Settings （全局设置）（续）

属性	描述
Direct connection for Offline Desktop operations （Offline Desktop 操作采用直接连接）	对于基于 LAN 的数据传输， Offline Desktop （如果可用）支持安全加密链路通信或非安全加密链路通信。 启用安全加密链路时，所有流量均通过 View Connection Server 进行传送。未启用安全加密链路时，直接在联机桌面主机系统与脱机客户端之间传输数据。
Use SSL for Offline Desktop operations （使用 SSL 执行 Offline Desktop 操作）	确定是否对 Offline Desktop 客户端与 View Connection Server 之间的通信和数据传输进行加密。
Disable Single Sign-On for Offline Desktop operations （对 Offline Desktop 操作禁用单点登录）	确定是否为 Offline Desktop 启用单点登录。禁用后，用户必须手动登录到桌面，才可启动 Windows 会话。
Display a pre-login message （显示登录前的消息）	确定 View Client 和 View Portal 用户能否看到一条免责声明或登录消息，其中包含管理员在显示的字段中输入的信息或说明。
Display a warning before forced logoff （强制注销前显示警告）	确定在计划或即时的更新事件 （例如，桌面刷新）之后是否注销桌面用户。 在显示的字段中，输入要显示的通知消息，以及显示此消息与用户注销之间的时间间隔。

事件视图

使用 [Events （事件）] 视图可以检查 View Connection Server 内执行的操作所生成的事件。您可以在 [Contains （包含）] 字段中输入文本，并根据消息类型、消息发布时间或消息文本本身进行搜索。此外，您还可以确定要显示消息的天数。使用 **[Events （事件）]** 页面中的信息，您可诊断问题或查看服务器上的活动。

搜索事件

1 单击 **[Messages contains （消息包含）]** 之后的箭头，并选择要搜索的列 （**[Messages （消息）]**、 **[Time （时间）]**、 **[Type （类型）]**）。

2 从列表中，选择要在 [Events （事件）] 表中显示消息的天数，然后单击 **[Done （完成）]**。

3 在文本框中输入搜索文本，然后单击 **[Find （查找）]**。

[Events （事件）] 表中随即显示搜索结果。单击每条消息结尾处的 **[(more...) （更多……）]**，可显示该事件的详细信息。

虚拟桌面部署

4

虚拟桌面部署是指准备单个或多个虚拟机的任务，以便 View Manager 客户端连接到虚拟机。部署虚拟桌面后，就可以直接访问已准备好的系统，或将它们作为模板使用，以便 View Manager 从中创建可扩展的克隆桌面池。

本章讲述桌面部署的端到端要求以及相关操作，并集中阐述如何使用 vCenter Server 管理的虚拟机创建桌面和桌面池。

本章讲述以下主题：

虚拟桌面部署概述

部署虚拟桌面步骤的不同取决于您是想创建由模板生成的自动池、单独的桌面实例，还是手动桌面池。但是，无论在何种情况下，都必须先选择一个基础系统或客户系统，并将其配置为与 View Manager 结合使用。

桌面源

不同的桌面源提供不同的应用程序支持和用户体验。桌面源的配置和管理方式及其提供的部署选项也有所不同。 View Manager 支持以下桌面源：

由 View Manager 部署并由 vCenter Server 管理的桌面源：此类桌面源是指由 View Manager 部署、并由 vCenter Server 管理的虚拟机。要添加此类桌面源，管理员必须指定以下设置：

- 用于部署和管理虚拟机的 vCenter Server。您只能使用 View Manager 服务器可识别的 vCenter Server。
- 用于部署虚拟机的模板。
- vCenter Server 清单层次结构中用于添加虚拟机的位置。
- 用于虚拟机的数据存储。
- 用于虚拟机的自定义规范。

非 View Manager 部署、但由 vCenter Server 管理的桌面源：此类桌面源是指由 vCenter Server 管理、并非 View Manager 部署的虚拟机。虚拟机已驻留在 vCenter Server 中。要添加此类桌面源，管理员必须指定以下设置：

- 用于管理虚拟机的 vCenter Server。您只能使用 View Manager 服务器可识别的 vCenter Server。
- 单个桌面：选择一个虚拟机，并将其添加为桌面源。
- 桌面池：选择多个虚拟机，并将它们添加为桌面源。
- 如果虚拟机已分配给其他桌面，则会显示错误。您必须从先前分配的桌面池或单个桌面中删除该桌面。

未被管理的桌面源：此类桌面源是指不受 vCenter Server 管理的计算机。这包括 VMware Server 中运行的虚拟机，以及支持 View Agent 的其他虚拟化平台中运行的虚拟机。可用来安装 View Agent 的刀片 PC、物理 PC 和终端服务器都是未被管理的桌面源。

桌面交付模式

统一访问支持各种不同的桌面交付模式，这些模式用于确定如何创建、授权、交付和使用桌面。 View Manager 支持以下桌面交付模式：

单个桌面：指具有以下特征、且支持单个预先存在的后端源的桌面：

- 可授权给多个用户或用户组，但每次只能授权给一名活动用户。
- 不会自动部署。

手动池：指具有以下特征的桌面源的池：

- 多个用户将映射到多个桌面，但每次只能有一个处于活动状态的用户映射到一个桌面。
- 不会自动部署。
- 支持永久和非永久的访问模式。
- 管理员可将整个池授权给用户或用户组。

自动池：指包含一个或多个动态生成的桌面的池，这些桌面是 View Manager 通过 vCenter Server 虚拟机模板自动创建并自定义的，它们具有以下特征：

- 多个用户将映射到多个桌面，但每次只能有一个处于活动状态的用户映射到一个桌面。
- 自动进行部署。
- 由管理员指定用于部署桌面源的模板和自定义规范。
- 支持永久和非永久的访问模式。
- 管理员可将整个池授权给用户或用户组。

终端服务器池：指由一台或多台终端服务器提供服务的终端服务器 （TS）桌面源组成的池。终端服务器桌面源可交付多个桌面。 TS 池具有以下特征：

- TS 桌面池由含有一个或多个终端服务器的服务器农场提供服务。
- 负载平衡基于最小会话计数：即选择具有最小活动会话计数的池之后，在该池内所有终端服务器之间的 View Manager 负载平衡连接请求数目。
- 管理员可将整个池授权给用户或用户组。
- 管理员应部署漫游配置文件解决方案，以便将用户设置及个性化设置传播到当前访问的桌面。

注释 终端服务器桌面池仅支持 RDP 显示协议。

准备客户系统

您在 vCenter 中所创建虚拟机的客户系统是部署虚拟桌面的基础。虚拟机必须符合第 14 页上的 “系统要求” 中描述的要求。

要准备客户系统以便部署，请执行以下任务：

- 按照 VMware vSphere 文档中的描述安装客户操作系统。如果要安装 Windows XP 作为客户操作系统，请访问以下网站，查看《Windows XP Deployment Guide》（Windows XP 部署指南）中的其他说明和指导：

  http://www.vmware.com/files/pdf/resources/
  vmware-view-xp-deployment-guide.pdf

- 安装最新版本的 VMware Tools （随 VMware vSphere 提供）。
- 安装 Microsoft 服务包和 Windows 更新。
- 安装防病毒软件。
- 安装其他应用程序，例如 Windows Media Player （如果您使用 MMR）。
- 安装所需的智能卡 （如通用存取卡）驱动程序。
- 配置网络代理设置。
- 配置 Active Directory 设置。

  a 用您的 Active Directory 服务器地址配置您的首选及备用 DNS 服务器的地址。

  例如，在 Windows XP 上，可使用属性菜单配置 DNS 服务器设置：

  [Start （开始）] > [Control Panel （控制面板）] > [Network Connections （网络连接）] > [LAN] > [Properties （属性）] > [Internet Protocol (TCP/IP) （Internet 协议 (TCP/IP)）] > [Properties （属性）] > [Use the following DNS server addresses （使用下面的 DNS 服务器地址）]

  b 将客户系统加入到适当的 Active Directory 域。

- 如果客户系统带有多个虚拟网卡，您必须配置 View Agent 要使用的子网。有关更多信息，请参阅第 68 页上的 “在带有多个虚拟网卡的虚拟机中使用 View Agent” 。
- 将防火墙配置为允许远程桌面连接。
- 请确保您拥有该客户系统的管理权限。
- （可选）配置用户自定义脚本。
- （可选）按照《Windows XP Deployment Guide》（Windows XP 部署指南）中有关性能优化的指导信息进行操作。

在客户系统中安装 View Agent

必须在客户系统上安装 View Agent，然后 View Connection Server 才能与虚拟桌面进行通信。

安装 View Agent

1 在客户系统上运行以下可执行文件，其中 xxxxxx 是该文件的内部版本号：

```
VMware-viewagent-xxxxxx.exe
```

2 显示 VMware 安装向导时，请单击 **[Next （下一步）]**。

3 接受 VMware 许可条款并单击 **[Next （下一步）]**。

4 选择自定义的安装选项。

如果要部署链接克隆桌面，则必须安装 **View Composer Agent**。有关此功能的更多信息，请参阅第 121 页上的第 6 章，“View Composer”。

您还可以选择或取消选择以下功能：

- 如果您希望允许用户从 View Connection Server 下载虚拟桌面的副本，以便在笔记本电脑等本地计算机上使用，请安装 **Offline Desktop** 组件。

  vSphere 4 不支持 Offline Desktop。Offline Desktop 是一项试验性功能。有关试验性功能的详细信息，请参阅第 14 页上的 “系统要求”。

- 如果虚拟桌面用户需要使用虚拟桌面访问本地连接的 USB 设备，请安装 **USB Redirection** 组件。

  注释 Windows 2000 不支持 USB 重定向。

- 如果要启用单点登录 （Single Sign-on， SSO），请安装 **View Secure Authentication** 组件。

  如果启用了该功能，用户在登录 View Client 时不会收到重新输入身份验证信息的提示，即可登录到虚拟桌面。

- 如果在事先未安装其他驱动的情况下，让用户在虚拟桌面使用客户系统的打印机，请安装 **Virtual Printing** 组件。请参阅第 112 页上的 “虚拟打印”。

- 如果希望允许用户通过 PCoIP 显示协议进行连接，请安装 **PCoIP Server** 组件。 PCoIP 为 LAN 或 WAN 中的广大用户提供图像、音频和视频内容传送方面的最佳 PC 体验。

注释 在 Windows Vista 中，如果您安装了 **PCoIP Server** 组件， Windows 组策略 **[Disable or enable software Secure Attention Sequence （禁用或启用软件安全注意序列）]** 将被启用并设置为 [`Services and Ease of Access applications` （服务和轻松访问应用程序）]。如果更改此设置，单点登录功能将无法正常工作。

5 接受或更改目标文件夹，并单击 **[Next （下一步）]**。

6 请单击 **[Install （安装）]** 开始安装。

7 完成安装后，单击 **[Finish （完成）]**。

在带有多个虚拟网卡的虚拟机中使用 View Agent

对于带有多个虚拟网卡的客户系统，您必须配置 View Agent 要使用的子网。它将确定 View Agent 向 View Connection Server 提供的、用于客户端 RDP 连接的网络地址。

要配置该子网，请在安装 View Agent 的虚拟机中创建以下注册表字符串，其中 `n.n.n.n` 是指 TCP/IP 子网，而 `m` 是指子网掩码中的位数：

```
HKLM\Software\VMware Inc.\VMware VDM\Node Manager\subnet = n.n.n.n/m (REG_SZ)
```

单个桌面

单个桌面是指包含 View Agent、且可以由 View Manager 客户端进行远程访问的单个虚拟机。有权使用此类桌面的用户，将在每次连接时始终访问同一系统。

单个桌面适用于那些需要唯一专用桌面的用户，也适用于使用单个主机许可证安装一款成本高昂、需由多名用户在不同时间进行访问的应用程序的情况。

单个桌面并不是永久分配给特定用户的，可以将其授权给多个用户进行访问。因此，其使用模式与经过认证的多个用户所共享的物理系统完全相同。

部署单个桌面

1 在 [View Administrator] 界面中单击 **[Desktops and Pools （桌面和池）]** 按钮，然后单击 **[Inventory （清单）]** 选项卡。在 **[Desktops （桌面）]** 窗格中，请确保选中 **[Desktops and Pools （桌面和池）]** 选项卡，并单击 **[Add （添加）]**。

2 随即显示 [Add Desktop （添加桌面）] 向导。在此向导中，您可以配置和部署新的链接克隆桌面池。选择 **[Individual Desktop （单个桌面）]**，并单击 **[Next （下一步）]**。

3 选择 **[vCenter virtual machine （vCenter 虚拟机）]** 或 **[Other sources （其他源）]**，指定客户系统的源类型。单击 **[Next （下一步）]**。

4 仅在选择了某个虚拟机作为客户系统后，才会显示此步骤。从显示的列表中，选择此桌面要使用的 vCenter Server。单击 **[Next （下一步）]**。

5 输入 **[Unique ID （唯一 ID）]**，也可以输入 **[Display name （显示名称）]** 和 **[Description （描述）]**。

唯一 ID 是 View Manager 用来识别桌面池的标识，也是客户端在登录时看到的名称。您可随意指定唯一 ID 和显示名称，如果未指定显示名称，系统会将唯一 ID 同时用作显示名称。如果有多个 VirtualCenter 或 vCenter Server，请参见第 201 页上的 "唯一 ID 的唯一性"。

注释 对于可选描述，您可以使用包括空格在内的任何字母数字字符。描述最多可为 1024 个字符，且只能在 View Administrator 中显示。

提供桌面标识的详细信息后，请单击 **[Next （下一步）]**。

6 配置桌面属性，并单击 **[Next （下一步）]**。

属性	参数描述
State （状态）	**[Enabled （启用）]** – 创建桌面池后，自动启用桌面池并准备立即使用。 **[Disabled （禁用）]** – 创建桌面池后，即禁用桌面池。如果要执行部署后的活动，如测试或其他形式的基准维护，则该设置很适用。
When VM is not in use （未使用虚拟机时）	**[Do nothing (VM remains on) （不执行任何操作 （虚拟机始终开机））]** – 您可根据需要启动已关机的虚拟机并保持开机状态，即使在不使用时亦如此，直到关机为止。 **[Always on (ensure VM is always powered on) （始终开机 （确保虚拟机始终开机））]** – 池中所有虚拟机始终保持开机，即使在不使用它们时亦如此。如果虚拟机已关机，则系统将立即重新启动该虚拟机。 **[Suspend VM （挂起虚拟机）]** – 不使用时，池中所有虚拟机都处于挂起状态。 **[Power off VM （关闭虚拟机）]** – 不使用时，池中所有虚拟机都将关机。 第 169 页上的 "电源策略" 中详细介绍了电源策略。
Automatic logoff after disconnect （断开连接后自动注销）	仅在选择了某个虚拟机作为客户系统后，才会显示此选项。 **[Immediately （立即）]** – 用户在断开连接后立即注销。 **[Never （永不）]** – 永不注销用户。 **[After （之后）]** – 指用户断开连接后，在此时间过后即注销用户。请在显示的字段中输入持续时间 （以分钟为单位）。

属性	参数描述
Allow users to reset their desktop （允许用户重置桌面）	如果要允许桌面用户在没有管理员协助的情况下重置其桌面，请选择此属性。
Default display protocol （默认显示协议）	选择您希望 View Connection Server 与 View Client 通信时使用的显示协议。 **PCoIP** – 可为 LAN 或 WAN 中的广大用户提供图像、音频和视频内容传送方面的最佳 PC 体验。 PCoIP 可以作为虚拟机和使用 Teradici 主机卡的物理机的单独桌面的显示协议。 **Microsoft RDP** – 一种允许用户连接到运行 Microsoft RDC 的计算机的多通道协议。 **HP RGS** – 请参见第 118 页上的 "使用 HP RGS 显示协议"。 HP RGS 可充当 HP Blade PC、 HP Workstation 和 HP Blade Workstation 的显示协议，但不适用于虚拟机。
Allow users to override the default protocol （允许用户重写默认协议）	如果希望桌面用户可以从 View Client 中重写默认的显示协议设置，请选择此属性。
Max number of monitors （显示器最大数量）	如果使用 PCoIP，请选择用户可用于显示桌面的显示器的最大数量。 **注释：**您必须关闭然后再启动现有虚拟机，才能使该设置生效。
Resolution of each monitor （每台显示器的分辨率）	如果使用 PCoIP，请选择分辨率最高的显示器的像素尺寸。 **注释：**您必须关闭然后再启动现有虚拟机，才能使该设置生效。
Adobe Flash quality （Adobe Flash 质量）	从下拉菜单中，选择 View Client 中显示的 Adobe Flash 动画的质量级别。低的质量级别可在较低带宽的情况下有更快的显示刷新速度。
Adobe Flash throttling （Adobe Flash 调节）	从下拉菜单中，选择 View Client 中显示的 Adobe Flash 动画的调节级别。较高的调节级别，在较低带宽的时候会使动画的帧速率下降。

注释 检入桌面之前，脱机桌面的属性设置不会生效。

警告 如果使用 Windows Vista 虚拟机，则*必须*将电源策略设置为 **[Ensure VM is always powered on （确保虚拟机始终开机）]**。

7 从显示的列表中，选择要用作单个桌面的虚拟机或物理机，然后单击 **[Next （下一步）]**。

8 随即显示此部署的配置设置摘要。

- 如果您对配置的任何内容不满意，可以使用 **[Back （返回）]** 按钮重新访问先前的任何页面。
- 如果您对配置很满意，请单击 **[Finish （完成）]** 以部署单个桌面。

启动部署之后，您可以选择 [Global desktop and pool view （全局桌面和池视图）] 窗格中的 **[Desktops and Pools （桌面和池）]** 或 **[Desktop Sources （桌面源）]** 选项卡来监控单个桌面的部署进度。

自动桌面池

自动桌面池包含一个或多个动态生成的桌面，这些桌面是 View Manager 通过 vCenter Server 虚拟机模板自动创建并自定义的。此类桌面池包括：

- 永久型：这种类型的桌面池中的桌面都是静态分配的，以确保用户每次登录时都能连接到同一系统。在用户首次连接时，就会进行桌面分配。
- 非永久 – 此类池中的桌面是在用户登录时动态分配的，并在用户断开连接时返回到池中。

自动桌面池可以使用链接克隆功能从单个 "父虚拟机" 中快速部署桌面。但是，本部分介绍的部署不使用此功能。有关链接克隆及其部署过程的更多信息，请参阅第 121 页上的第 6 章， "View Composer"。

虚拟机模板

安装并配置客户系统后，将虚拟机转换为一个模板。随后，您可以将该模板用作自动桌面池的桌面源。

View Composer 链接克隆虚拟桌面使用快照 （而不是虚拟机模板）作为基础映像。请参阅第 121 页上的第 6 章， "View Composer"。

在 vCenter 中创建虚拟机模板

1 关闭虚拟机。

2 右键单击以前配置的客户系统，然后选择下列选项之一：

- **[Clone to Template （克隆到模板）]**：如果要在不更改虚拟机本身的情况下使用选定的客户系统作为新模板的基础，请选择此选项。如果选择此选项，系统将显示设置向导，要求您提供模板名称、模板所在位置的相关环境信息，以及要使用的磁盘格式。
- **[Convert to Template （转换为模板）]**：如果要将客户系统更改为模板，请使用此选项。此转换过程非常迅速。

自定义规范

自定义规范是可选步骤。但是，通过为许可、域附属和 DHCP 设置等常规属性提供配置信息，这些自定义规范可显著加快自动桌面池的部署速度。

创建自定义规范

1. 在 vCenter Server 中，单击 **[Edit （编辑）]** > **[Customization Specifications （自定义规范）]**。
2. 单击 **[New （新建）]** 以创建新的自定义规范。
3. 请确保选中 **[Target Virtual Machine OS （目标虚拟机操作系统）]** 下拉菜单中的 **[Windows]**，并在显示的字段中，输入自定义规范的名称和 （可选）描述。单击 **[Next （下一步）]**。
4. 输入要与您在显示字段内自动池中创建的桌面相关联的 **[Name （名称）]** 和 **[Organization （单位）]**。单击 **[Next （下一步）]** 以继续。
5. 选择以下选项之一：
   - **[Use the virtual machine name （使用虚拟机名）]**：在从 View Manager 中进行部署的过程中，如果需要池中的桌面从分配给每个桌面虚拟机的名称中派生名称，则可以选择此选项。此选项为建议选项。
   - **[Use a specific name （使用特定名称）]**：如果需要每个桌面从预定义的标签中派生名称，则可选择此选项。如果选择此选项，建议您还应选中 **[Append a numeric value to ensure uniqueness （附加数字值以确保唯一性）]**。

   单击 **[Next （下一步）]**。
6. 在 **[Product ID （产品 ID）]** 字段中，输入 View Manager 桌面操作系统的许可证编号，并指定它是单个还是多个 seat 许可证。单击 **[Next （下一步）]**。
7. 在显示的字段中输入并确认本地管理员密码。单击 **[Next （下一步）]**。
8. 从下拉列表中选择本地时区。单击 **[Next （下一步）]**。
9. （可选）您可提供一个或多个命令提示说明，用户首次连接时将执行这些说明。在显示的字段中输入一条命令，并单击 **[Add （添加）]**。必要时可重复此步骤。

   完成后，请单击 **[Next （下一步）]**。
10. 为网络接口指定要使用的设置类型。建议选项为 **[Typical settings （典型设置）]**。单击 **[Next （下一步）]**。

11 指定如何从该模板中派生网络中要包含的桌面。

如果要将已部署的桌面自动添加到域，请选择 **[Windows Server Domain（Windows Server 域）]**，并在显示的字段中输入适当的名称。在 [Username（用户名）]、[Password（密码）] 和 [Password confirmation（密码确认）] 字段中，输入具有必要权限级别的用户凭据，以便将系统添加到该域。

12 确保已选中 **[Generate New Security ID (SID)（生成新的安全 ID（SID））]**，并单击 **[Next（下一步）]**。

部署自动桌面池

1 在 View Administrator 中单击 **[Desktops and Pools（桌面和池）]** 按钮，然后单击 **[Inventory（清单）]** 选项卡。在 [Global desktop and pool view（全局桌面和池视图）] 窗格中，请确保选中 **[Desktops and Pools（桌面和池）]** 选项卡，并单击 **[Add（添加）]**。

2 随即显示 [Add Desktop（添加桌面）] 向导。在此向导中，您可以配置和部署新的链接克隆桌面池。选择 **[Automated Desktop Pool（自动桌面池）]**，并单击 **[Next（下一步）]**。

3 选择要创建的桌面池类型，并单击 **[Next（下一步）]**。

池类型	描述
Persistent（永久）	这种类型的桌面池中的桌面是静态分配的，以确保用户每次登录时都能连接到同一系统。在用户首次连接时，就会进行桌面分配。
Non-persistent（非永久）	此类池中的桌面是在用户登录时以动态方式分配的，并在用户断开连接时返回到池中。

4 从显示的列表中，选择此桌面要使用的 vCenter Server。单击 **[Next（下一步）]**。

5 输入 **[Unique ID（唯一 ID）]**，也可以输入 **[Display name（显示名称）]** 和 **[Description（描述）]**，然后单击 **[Next（下一步）]**。

唯一 ID 是 View Manager 用来识别桌面池的标识，也是用户在登录时看到的名称。您可随意指定唯一 ID 和显示名称，如果未指定显示名称，系统会将唯一 ID 同时用作显示名称。如果有多个 VirtualCenter 或 vCenter Server，请参见第 201 页上的 "唯一 ID 的唯一性"。

对于可选描述，您可以使用包括空格在内的任何字母数字字符。描述最多可为 1024 个字符，且只能在 View Administrator 中显示。

6 配置桌面属性，并单击 **[Next （下一步）]**。

> **警告** 如果使用 Windows Vista 虚拟机，则*必须*将电源策略设置为 **[Ensure VM is always powered on （确保虚拟机始终开机）]**。

属性	参数描述
State （状态）	**[Enabled （启用）]** – 创建桌面池后，自动启用桌面池并准备立即使用。 **[Disabled （禁用）]** – 创建桌面池后，即禁用桌面池。如果要执行部署后的活动，如测试或其他形式的基准维护，则该设置很适用。
When VM is not in use （未使用虚拟机时）	**[Do nothing (VM remains on) （不执行任何操作 （虚拟机始终开机））]** – 您可根据需要启动已关机的虚拟机并保持开机状态，即使在不使用时也是如此，直到关机为止。 **[Always on (ensure VM is always powered on) （始终开机 （确保虚拟机始终开机））]** – 池中所有虚拟机始终保持开机状态，即使不使用它们时也是如此。如果虚拟机已关机，则系统将立即重新启动该虚拟机。 **[Suspend VM （挂起虚拟机）]** – 池中所有虚拟机在不使用时都处于挂起状态。 **[Power off VM （关闭虚拟机）]** – 池中所有虚拟机在不使用时都将关机。 第 169 页上的 "电源策略" 中详细介绍了电源策略。
Automatic logoff after disconnect （断开连接后自动注销）	**[Immediately （立即）]** – 用户在断开连接后立即注销。 **[Never （永不）]** – 永不注销用户。 **[After （之后）]** – 指用户断开连接后，在此时间过后即注销用户。请在显示的字段中输入持续时间 （以分钟为单位）。
Power off and delete virtual machine after first use （首次使用后关闭并删除虚拟机） （仅限于非永久池）	要在用户注销后立即删除虚拟机，请选择此属性。 如有必要，在删除虚拟机后，可以克隆新虚拟机以维护特定池的大小。
Allow users to reset their desktop （允许用户重置桌面）	如果要允许桌面用户在没有管理员协助的情况下重置其桌面，请选择此属性。

属性	参数描述
Allow multiple sessions per user （允许每个用户多个会话） （仅限于非永久池）	如果要支持各个用户同时连接到同一池中的多个桌面，请选中此属性。
Default display protocol （默认显示协议）	选择您希望 View Connection Server 与 View Client 通信时使用的显示协议。 **PCoIP** – 可为 LAN 或 WAN 中的广大用户提供图像、音频和视频内容传送方面的最佳 PC 体验。 **Microsoft RDP** – 一种允许用户连接到运行 Microsoft RDC 的计算机的多通道协议。
Allow users to override the default protocol （允许用户重写默认协议）	如果希望桌面用户可以在 View Client 中重写默认显示协议，请选择此属性。
Max number of monitors （显示器最大数量）	如果使用 PCoIP，请选择用户可用于显示桌面的显示器的最大数量。 **注释：**您必须关闭然后再启动现有虚拟机，才能使该设置生效。
Resolution of each monitor （每台显示器的分辨率）	如果使用 PCoIP，请选择分辨率最高的显示器的像素尺寸。 **注释：**您必须关闭然后再启动现有虚拟机，才能使该设置生效。
Adobe Flash quality （Adobe Flash 质量）	从下拉菜单中，选择 View Client 中显示的 Adobe Flash 动画的质量级别。低的质量级别可在较低带宽的情况下有更快的显示刷新速度。
Adobe Flash throttling （Adobe Flash 调节）	从下拉菜单中，选择 View Client 中显示的 Adobe Flash 动画的调节级别。较高的调节级别，在较低带宽的时候会使动画的帧速率下降。

7 配置桌面部署属性，并单击 **[Next （下一步）]**。

属性	参数描述
Provisioning （部署）	**[Enabled （启用）]**：完成部署步骤或删除桌面后立即在池中创建桌面。 **[Disabled （禁用）]**：完成部署步骤或删除桌面后不立即在池中创建桌面。
Number of desktops （桌面数）	指定要在该池中创建的桌面数。如果选中 **[Advanced Settings（高级设置）]** 面板中的 **[Enable Advanced Pool Settings （启用高级池设置）]**，则会禁用此设置。

VM naming pattern （虚拟机命名模式）	默认情况下，前缀用来标识属于某一池中相同组的所有桌面。前缀最多为 13 个字符，并附有一个数字后缀，以便将相同池中的每个桌面逐一加以区别。
	通过输入一个包含表示池编号的令牌名称，可以重写此行为，该令牌在任何位置均以相同方式显示。例如：
	`amber-{n}-desktop`
	部署后，系统将使用桌面的池编号替换 `{n}`。
	您可使用 `n:fixed=` 结构输入固定长度的令牌。例如：
	`amber-{n:fixed=3}`
	部署后，系统将使用每个桌面的固定长度池编号替换 `{n:fixed=3}`：`amber-001`、 `amber-002` 和 `amber-003` 等。
	包含令牌且采用固定令牌长度替换的名称最多只能使用 15 个字符。例如：
	`my-view-system{n:fixed=1}`
	其中，令牌长度不固定，其缓冲值为 1，因此，最大 “替换” 长度为 14 个字符。例如：
	`a-view-system{n}`

Stop provisioning on error （出错时停止部署）	如果在创建桌面过程中检测到错误，且需要 View Manager 自动停止部署新虚拟机，请选中此属性。
Advanced Settings （高级设置）	单击可显示高级池配置设置。通过选中 **[Enable Advanced Pool Settings （启用高级池设置）]**，可以启用高级参数。此选项将禁用 **[Pool Size （池大小）]** 参数。 **[Minimum number of virtual machines （最小虚拟机数）]**：指必须为该池部署的最小桌面数。 **[Maximum number of virtual machines （最大虚拟机数）]**：指可以为该池部署的最大桌面数。 **[Number of available virtual machines （可用虚拟机数）]**：指不必分配的、在任何时候均可使用的虚拟机数。此数字不可超过整个池中的最大可用桌面数。

8 选择要作为部署基础映像的模板。系统随即仅显示那些包含 View Manager 支持的桌面操作系统的模板。单击 **[Next （下一步）]**。

9 选择此桌面池的文件夹要在 vCenter Server 中驻留的位置，并单击 **[Next （下一步）]**。

10 选择要在其中运行此桌面使用的虚拟机的主机或群集，并单击 **[Next （下一步）]**。

注释 系统仅支持 8 台或更少主机的群集，并在屏幕中显示。

---

11 选择要在其中运行此桌面使用的虚拟机的资源池，并单击 **[Next （下一步）]**。

12 选择一个或多个要在其中存储桌面池的数据存储。如果可用空间不足，则您必须选择额外的数据存储以增加可用空间。

注释 对于群集，仅支持并显示共享数据存储。

配置数据存储的存储标准之后，请单击 **[Next （下一步）]**。

13 选择要从自定义的客户系统中创建桌面的方式。如果 vCenter Server 中存在自定义规范，则您可以从 **[Use this customization specification （使用此自定义规范）]** 列表中将其选中，以便预先配置许可、域附属和 DHCP 设置等属性。

如果要在部署桌面后手动配置该池中的桌面，或者如果未检测到任何自定义规范，请选中 **[None - Customization will be done manually （无 － 手动执行自定义）]**。

如果您希望虚拟机仍保持关机状态，还可选择 **[Do not power on virtual machines after creation （创建后不启动虚拟机）]**。

单击 **[Next （下一步）]**。

14 随即显示此部署的配置设置摘要。

- 如果您对配置的任何内容不满意，可以使用 **[Back （返回）]** 按钮重新访问先前的任何页面。
- 如果您对配置很满意，请单击 **[Finish （完成）]** 以部署自动桌面池。

启动部署后，您可以选择 [Global desktop and pool view （全局桌面和池视图）] 窗格中的 **[Desktops and Pools （桌面和池）]** 或 **[Desktop Sources （桌面源）]** 选项卡来监控自动桌面池的部署进度。

手动桌面池

手动桌面池是指 View Manager 管理员手动构建的虚拟机池。此类桌面池包括：

- 永久桌面池：指为用户分配一个保留会话之间所有文档、应用程序和设置的专用桌面。此类桌面是在用户首次连接时以静态方式分配的，稍后可用于所有后续会话。
- 非永久桌面池：指用户在每次连接时均连接到池中不同的桌面，且会话之间没有任何永久性的环境或用户数据。

部署手动桌面池

1 在 View Administrator 中单击 **[Desktops and Pools （桌面和池）]** 按钮，然后单击 **[Inventory （清单）]** 选项卡。在 [Global desktop and pool view （全局桌面和池视图）] 窗格中，请确保选中 **[Desktops and Pools （桌面和池）]** 选项卡，并单击 **[Add （添加）]**。

2 随即显示 [Add Desktop （添加桌面）] 向导。在此向导中，您可以配置和部署新的链接克隆桌面池。选择 **[Manual Desktop Pool （手动桌面池）]**，并单击 **[Next （下一步）]**。

3 选择要创建的桌面池类型，并单击 **[Next （下一步）]**。

池类型	描述
Persistent （永久）	这种类型的桌面池中的桌面是静态分配的，以确保用户每次登录时都能连接到同一系统。在用户首次连接时，就会进行桌面分配。
Non-persistent （非永久）	此类池中的桌面是在用户登录时以动态方式分配的，并在用户断开连接时返回到池中。

4 选择 **[vCenter virtual machine （vCenter 虚拟机）]** 或 **[Other sources （其他源）]**，指定客户系统的源类型。单击 **[Next （下一步）]**。

5 从显示的列表中，选择此桌面要使用的 vCenter Server 服务器。单击 **[Next （下一步）]**。

6 输入 **[Unique ID （唯一 ID）]**，也可以输入 **[Display name （显示名称）]** 和 **[Description （描述）]**。

唯一 ID 是 View Manager 用来识别桌面池的标识，也是用户在登录时看到的名称。您可随意指定唯一 ID 和显示名称，如果未指定显示名称，系统会将唯一 ID 同时用作显示名称。如果有多个 VirtualCenter 或 vCenter Server，请参见第 201 页上的 "唯一 ID 的唯一性"。

注释 对于可选描述，您可以使用包括空格在内的任何字母数字字符。描述最多可为 1024 个字符，且只能在 View Administrator 中显示。

提供桌面标识的详细信息后，请单击 **[Next （下一步）]**。

7 配置桌面属性，并单击 **[Next （下一步）]**。

> **警告** 如果使用 Windows Vista 虚拟机，则*必须*将电源策略设置为 **[Ensure VM is always powered on （确保虚拟机始终开机）]**。

属性	参数描述
State （状态）	**[Enabled （启用）]** – 创建桌面池后，自动启用桌面池并准备立即使用。 **[Disabled （禁用）]** – 创建桌面池后，即禁用桌面池。如果要执行部署后的活动，如测试或其他形式的基准维护，则该设置很适用。
When VM is not in use （未使用虚拟机时） （仅限于虚拟机客户机）	**[Do nothing (VM remains on) （不执行任何操作 （虚拟机始终开机））]** – 您可根据需要启动已关机的虚拟机并保持开机状态，即使在不使用时也是如此，直到关机为止。 **[Always on (ensure VM is always powered on) （始终开机 （确保虚拟机始终开机））]** – 池中所有虚拟机始终保持开机状态，即使不使用它们时也是如此。如果虚拟机已关机，则系统将立即重新启动该虚拟机。 **[Suspend VM （挂起虚拟机）]** – 池中所有虚拟机在不使用时都处于挂起状态。 **[Power off VM （关闭虚拟机）]** – 池中所有虚拟机在不使用时都将关机。 第 169 页上的 "电源策略" 中详细介绍了电源策略。
Automatic logoff after disconnect （断开连接后自动注销）	**[Immediately （立即）]** – 用户在断开连接后立即注销。 **[Never （永不）]** – 永不注销用户。 **[After （之后）]** – 指用户断开连接后，在此时间过后即注销用户。请在显示的字段中输入持续时间 （以分钟为单位）。
Allow users to reset their desktop （允许用户重置桌面）	如果要允许桌面用户在没有管理员协助的情况下重置其桌面，请选择此属性。
Allow multiple sessions per user （允许每个用户多个会话） （仅限于非永久池）	如果要支持各个用户同时连接到同一池中的多个桌面，请选中此属性。

属性	参数描述
Default display protocol **（默认显示协议）**	选择您希望 View Connection Server 与 View Client 通信时使用的显示协议。 **PCoIP** － 可为 LAN 或 WAN 中的广大用户提供图像、音频和视频内容传送方面的最佳 PC 体验。 PCoIP 可以作为虚拟机和使用 Teradici 主机卡的物理机的手动桌面的显示协议。 **Microsoft RDP** － 一种允许用户连接到运行 Microsoft RDC 的计算机的多通道协议。 **HP RGS**：请参见第 118 页上的 "使用 HP RGS 显示协议"。 HP RGS 可充当 HP Blade PC、 HP Workstation 和 HP Blade Workstation 的显示协议，但不适用于虚拟机。
Allow users to override the default protocol **（允许用户重写默认协议）**	如果希望桌面用户可以在 View Client 中重写默认显示协议，请选择此属性。
Max number of monitors **（显示器最大数量）**	如果使用 PCoIP，请选择用户可用于显示桌面的显示器的最大数量。 **注释：**您必须关闭然后再启动现有虚拟机，才能使该设置生效。
Resolution of each monitor **（每台显示器的分辨率）**	如果使用 PCoIP，请选择分辨率最高的显示器的像素尺寸。 **注释：**您必须关闭然后再启动现有虚拟机，才能使该设置生效。
Adobe Flash quality **（Adobe Flash 质量）**	从下拉菜单中，选择 View Client 中显示的 Adobe Flash 动画的质量级别。低的质量级别可在较低带宽的情况下有更快的显示刷新速度。
Adobe Flash throttling **（Adobe Flash 调节）**	从下拉菜单中，选择 View Client 中显示的 Adobe Flash 动画的调节级别。较高的调节级别，在较低带宽的时候会使动画的帧速率下降。

注释 检入桌面之前，脱机桌面的属性设置不会生效。

8 从显示的列表中，选择要添加到池中的虚拟机或物理系统。单击 **[Next （下一步）]**。

9 随即显示此部署的配置设置摘要。

- 如果您对配置的任何内容不满意，可以使用 **[Back （返回）]** 按钮重新访问先前的任何页面。
- 如果您对配置很满意，请单击 **[Finish （完成）]** 以部署单个桌面。

启动部署之后，您可以选择 [Global desktop and pool view （全局桌面和池视图）] 窗格中的 **[Desktops and Pools （桌面和池）]** 或 **[Desktop Sources （桌面源）]** 选项卡来监控手动桌面池的部署进度。

授权桌面或池

创建桌面或桌面池之后，您可以授权 Active Directory 用户或用户组进行访问。

将桌面授权给 Active Directory 用户或用户组

1 在 View Administrator 中单击 **[Desktops and Pools （桌面和池）]** 按钮，然后单击 **[Inventory （清单）]** 选项卡下的 **[Global desktop and pool view （全局桌面和池视图）]** 条目。从 [Global desktop and pool view（全局桌面和池视图）] 窗格中选择要授权的桌面或池。

2 单击 **[Entitlements （授权）]**。随即显示 [Entitlements （授权）] 窗口，该窗口中列出可以使用此桌面或池的用户和用户组。单击 **[Add （添加）]**。

3 随即显示 [User and group entitlement （用户和用户组授权）] 窗口。从该窗口中，您可以查看、搜索和过滤该域林内的所有 Active Directory 用户。

4 在 **[Type （类型）]** 中，选中 **[Users （用户）]** 和 / 或 **[Groups （用户组）]**。

5 从 **[Domain （域）]** 下拉菜单中，选择包含要授权的用户或用户组的域，或选择 **[Entire Directory （完整目录）]** 以搜索整个 Active Directory 域林。

6 使用显示的字段，您可以按名称或描述进行搜索。单击 **[Find （查找）]** 执行搜索。

注释 如果要查看域中的所有用户列表，请将 **[Name （名称）]** 和 **[Description （描述）]** 字段保留为空。

---

7 在此表中，选择您希望可以使用此桌面或池的用户或用户组，并单击 **[OK （确定）]**。

8 您将返回至 [Entitlements （授权）] 窗口的首页，现在，该页面将显示您选择的用户或用户组。单击 **[OK （确定）]** 以完成操作。

限制 View 桌面访问

您可以使用受限制的授权功能，根据用户连接的 View Connection Server 实例限制 View 桌面访问。

使用受限制的授权功能，您可以为一个 View Connection Server 实例分配一个或多个标签。在之后配置桌面或桌面池时，您可以选择希望其能够访问桌面或桌面池的 View Connection Server 实例的标签。当用户通过带标签的 View Connection Server 实例登录时，他们可以只访问那些没有标签或至少有一个匹配标签的桌面和桌面池。

例如，您的部署中可能包含两个 View Connection Server 实例。其中一个实例用于支持内部用户。另一个实例则与安全服务器配对，用于支持您的外部用户。为防止外部用户访问特定桌面，您可以采用以下操作设置受限制的授权：

- 将 “内部” 标签分配给支持内部用户的 View Connection Server 实例。
- 将 “外部” 标签分配给与安全服务器配对并支持外部用户的 View Connection Server 实例。
- 将 “内部” 标签分配给仅供内部用户访问的桌面和桌面池。

在本例中，外部用户无法看到带有 “内部” 标签的桌面和桌面池，因为他们是通过带有 “外部” 标签的 View Connection Server 登录的。

同样，您可以使用受限制的授权功能，根据您为特定 View Connection Server 实例配置的用户身份验证方法控制桌面访问。例如，您可以仅允许经过智能卡身份验证的用户使用特定的桌面。

受限制的授权功能只能强制执行标签匹配。您必须设计网络拓扑结构已强制特定的客户端通过特定的 View Connection Server 实例进行连接。

了解标签匹配

受限制的授权功能通过标签匹配的方法来确定 View Connection Server 实例能否访问特定的 View 桌面或桌面池。

从最基本的层面来看，标签匹配方法可确定带有特定标签的 View Connection Server 实例能否访问带有相同标签的桌面或桌面池。

如果未分配标签，还会影响到 View Connection Server 实例能否访问桌面或桌面池。例如，不带有任何标签的 View Connection Server 实例只能访问同样不带任何标签的桌面和桌面池。

表 4-1 显示了受限制的授权功能如何确定 View Connection Server 在哪些情况下能访问桌面或桌面池。

表 4-1. 标签匹配规则

View Connection Server	桌面 / 桌面池	是否允许访问
无标签	无标签	是
无标签	一个或多个标签	否
一个或多个标签	无标签	是
一个或多个标签	一个或多个标签	仅标签匹配时允许访问

考虑因素与限制因素

单个 View Connection Server 实例、桌面或桌面池可以有多个标签。多个 View Connection Server 实例、桌面和桌面池可以有相同的标签。

不带任何标签的桌面和桌面池可被任何 View Connection Server 实例访问。不带任何标签的 View Connection Server 实例只能访问同样不带任何标签的桌面和桌面池。

如果使用安全服务器，必须在与其配对的 View Connection Server 实例上配置受限制的授权。您无法在安全服务器上配置受限制的授权。

如果 View Connection Server 实例的标签已被分配到桌面或桌面池，且不存在带有匹配标签的其他 View Connection Server 实例，则您无法修改或删除这些标签。

受限制的授权优先于其他桌面授权。例如，即使用户已获得访问某个桌面的权限，但如果这个桌面的标签与用户连接的 View Connection Server 实例所带的标签不匹配，用户也无法访问此桌面。

限制 View Connection Server 实例

当您向 View Connection Server 实例分配标签后，与该 View Connection Server 连接的用户只能访问带有匹配标签或不带标签的 View 桌面和桌面池。

为 View Connection Server 实例分配标签

1 在 View Administrator 中，选择 **[Configuration （配置）]** > **[Servers （服务器）]** > **[View Server]**。

2 选择 [View Connection Server] 实例并单击 **[Edit （编辑）]**。

3 在 [Tags （标签）] 字段中键入一个或多个标签。用逗号或分号分隔多个标签。

4 单击 **[OK （确定）]** 保存更改。

限制 View 桌面或桌面池

当您将标签分配给 View 桌面或桌面池后，只有连接到带有匹配标签的 View Connection Server 实例的用户才能访问此桌面或桌面池。您可以在添加或编辑桌面或桌面池时分配标签。

将标签分配给 View 桌面或桌面池

1 在 View Administrator 中，选择 **[Desktops and Pools（桌面和池）] > [Inventory（清单）] > [Global desktop and pool view （全局桌面和池视图）] > [Desktops and Pools （桌面和池）]**。

- 要为新的桌面或桌面池分配标签，请单击 **[Add （添加）]**。
- 要为现有的桌面或桌面池分配标签，请选择相应的桌面或桌面池，然后单击 **[Edit （编辑）]**。

2 在 **[Desktop/Pool Settings（桌面 / 池设置）]** 对话框内，选择 **[Connection server restrictions （连接服务器的限制）]** 下拉菜单。

- 单击 **[None （无）]**，可允许任何 View Connection Server 实例访问桌面或桌面池。
- 单击 **[With tags （带有标签的）]** 并选择一个或多个 View Connection Server 标签，可仅允许带有这些特定标签 （或不带标签）的 View Connection Server 实例访问桌面或桌面池。您可以按下 Ctrl+Shift 组合键选择多个标签。

3 单击 **[Done （完成）]** 保存更改。

搜索桌面和已授权的用户和用户组

使用 [Inventory （清单）] 选项卡搜索有关桌面和已授权用户和用户组的信息。您可以使用该页右侧表中的列进行搜索，也可以使用该页左侧的类别进行查找。

在 [Desktops Inventory （桌面清单）] 视图中搜索列

1 在 View Administrator 中，单击 **[Desktops and Pools （桌面和池）]** 按钮。

2 在 **[Desktops （桌面）]** 字段 （位于该页右侧）中，请单击 **[Desktops and Pools （桌面和池）]**、**[Desktop Sources（桌面源）]** 或 **[Active Sessions（活动会话）] 选项卡**。

3 单击 [Search （搜索）] 字段左侧的向下箭头，选中相应列的复选框。

4 单击 **[Done （完成）]**。

5 输入搜索文本，并单击 **[Go （搜索）]**。

在 [Desktops Search （桌面搜索）] 视图中搜索类别

1. 在 View Administrator 中单击 **[Desktops and Pools （桌面和池）]** 按钮，并单击位于该页左侧的 **[Search （搜索）]** 选项卡。
2. 在 **[Search for desktops and pools （搜索桌面和池）]** 字段中，输入搜索文本。
3. 选择或取消选择 **[Display Name （显示名称）]**、 **[Desktop ID （桌面 ID]**、 **[Type （类型）]**、 **[User （用户）]**、 **[Virtual Center name （Virtual Center 名称）]**、**[Desktop source（桌面源）]** 或 **[Persistence（永久）]**，以便在该类别中进行搜索。
4. 单击 **[Search （搜索）]**。

在 [Entitled Users and Groups Inventory （已授权的用户和用户组清单）] 视图中搜索列

1. 在 View Administrator 中，单击 **[Users and Groups （用户和用户组）]** 按钮。
2. 在 **[Global user and group view（全局用户和用户组视图）]** 字段（位于该页面右侧）中，单击 **[Entitled Users and Group （已授权的用户和用户组）]**、 **[Active Sessions （活动会话）]** 选项卡或（如果可用） **[Offline Sessions （脱机会话）]**。
3. 单击 [Search （搜索）] 字段左侧的向下箭头，选中相应列的复选框。
4. 单击 **[Done （完成）]**。
5. 输入搜索文本，并单击 **[Find （查找）]**。

在 [Entitled Users and Groups Search （已授权的用户和用户组搜索）] 视图中搜索类别：

1. 在 View Administrator 中，单击 **[Users and Groups （用户和用户组）]** 按钮，并单击位于该页左侧的 **[Search （搜索）]** 选项卡。
2. 在 **[Search for users and groups （搜索用户和用户组）]** 字段中，输入搜索文本。
3. 选择或取消选择 **[Name （名称）]**、 **[Email （电子邮件）]**、 **[Display name （显示名称）]** 或 **[Domain （域）]**，以便在该类别中进行搜索。
4. 单击 **[Search （搜索）]**。

使用活动会话

用户连接到桌面后，清单中将列出活动会话。您可以在 [Inventory （清单）] 页面中查看活动会话。

查看、断开或重新启动活动会话

1 在 View Administrator 中单击 **[Desktops and Pools （桌面和池）]** 按钮，并单击该页左侧的 **[Inventory （清单）]** 选项卡。

2 在 [Global desktop and pool view （全局桌面和池视图）] 中，单击 **[Active Sessions （活动会话）]**。在此视图中，您可以查看每个活动会话的用户、桌面 ID、 DNS 名称、开始时间、持续时间以及会话状态 （[connected （已连接）] 或 [disconnected （已断开）]）。

3 单击活动会话中的任何位置。 **[Disconnect Session （断开会话）]**、 **[Logoff Session （注销会话）]** 和 **[Reset Virtual Machine （重置虚拟机）]** 选项将变为活动状态。

选项	描述
Disconnect Session （断开会话）	用户已断开连接，但其会话仍处于活动状态。
Logoff Session （注销会话）	用户已断开连接，且其会话已注销。
Reset Virtual Machine （重置虚拟机）	在没有正常注销和断开的情况下关闭并重新启动桌面。

4 选择适当的选项，并在 [confirmation （确认）] 窗口中单击 **[OK （确定）]**。

禁用 View Manager 并删除对象

如果要阻止用户访问其桌面，可禁用 [View Connection Server] 以阻止客户端登录。禁用 [View Connection Server] 时，当前已登录的用户不受影响。

如果因任何原因需要停止 View Connection Server，禁用功能就很有用。禁用 [View Connection Server] 时，尝试登录的最终用户将看到一条消息，指出连接失败且当前已禁用 View Connection Server。

启用或禁用 View Connection Server 实例

1 单击 **[Configuration （配置）]** 按钮。

2 从服务器列表中选择 [View Connection Server]，并单击 **[Enable or Disable （启用或禁用）]**。

禁用 View Connection Server 不会影响当前的活动会话桌面，也不会阻止建立新的桌面会话。

删除 View Manager 对象

使用管理员用户界面，可以删除 View Manager 对象 （vCenter Server 连接、 View Connection Server 连接和桌面）。

从 View Connection Server 中删除 vCenter Server 连接

1 在 View Administrator 中，单击 **[Configuration （配置）]** 按钮。

2 在 **[vCenter Server]** 中，选择要删除的 VirtualCenter 或 vCenter Server，然后单击 **[Remove （删除）]。**

   如果某些桌面正在使用此 vCenter Server，则系统会显示一条错误消息，指出您必须先删除使用该 vCenter Server 的桌面，然后才可删除 vCenter Server。

   如果所有桌面均未使用 vCenter Server，则系统会显示一条警告消息，指出您无法再访问此 vCenter Server 管理的虚拟机。

3 单击 **[OK （确定）]**。

   vCenter Server 条目已被删除。

从 View Connection Server 中删除桌面池

1 在 View Administrator 中，单击 **[Desktops and Pools （桌面和池）]** 按钮。

2 在 [Global desktop and pool view （全局桌面和池视图）] 中，从右侧列表中选择桌面或桌面池，并单击 **[Delete （删除）]**。

   您可以选择仅从 View Manager 中删除虚拟机 （这意味着仍可在 vCenter Server 中看到虚拟机）；也可以从磁盘中将其删除 （将无法在 vCenter Server 中看到虚拟机）。

   如果桌面具有活动会话，您可以断开用户连接 （这意味着用户将丢失已连接的桌面）；也可以保留用户的连接状态 （用户不会丢失已连接的桌面）。

客户端管理 5

使用本地安装的 View Client 应用程序和基于 Web 的 View Portal 组件，用户就可以连接到他们的桌面。这些应用程序既可以在内部网络中运行，也可以通过 Internet 在外部网络中运行，而且您可以用多种方式修改其行为。

此外， View Client 还提供多种用户身份验证模式 （包括安全身份验证），但必须先在 View Connection Server 中配置所有这些模式。

注释 需要使用 View 的 Offline Desktop 试验性功能的用户必须使用 View Client with Offline Desktop，它支持本地 （脱机）和远程桌面访问。有关此功能的更多信息，请参阅第 157 页上的第 7 章， "Offline Desktop"。

本章讲述以下主题：

- 第 115 页上的 “客户端计算机信息”
- 第 118 页上的 “使用 PCoIP 显示协议”
- 第 118 页上的 “使用 HP RGS 显示协议”

注释 根据所使用的 View Client 的不同，您体验到的功能将有所不同。本指南主要介绍用于 Microsoft Windows 的 View Client 和 View Portal。本指南中，未详细介绍以下类型的客户端：

- 用于 Linux 的 View Portal （处于试验阶段）和用于 Mac OS X 的 View Portal （处于试验阶段）。
- 用于 Linux 的 View Client （仅通过认证的合作伙伴才可以使用）。
- 各种第三方客户端 （仅通过认证的合作伙伴才可以使用）。
- View Open Client（支持 VMware 合作伙伴认证计划）。View Open Client 不是官方的 View Client，因此不受支持。

安装和运行 View Client 与 View Portal

本部分介绍如何安装 View Client 与 View Portal 所需的组件。必须以管理员的身份登录到客户端系统，才能执行这些任务。

View Client 与 View Portal 提供的功能源于本地安装的一套基础组件。已安装 View Client 的用户首次使用 View Portal 时，系统会要求用户在浏览器中安装附加的 ActiveX 控件。

同样，未安装 View Client 的 View Portal 用户在首次联机时，系统会提示允许浏览器自动安装所需的 View Client 组件。

通过访问 View Portal 网页并允许浏览器在客户端系统中自动安装所需组件，就可以很便捷地安装 View Client 应用程序。不过，如果选择此安装方式，必须注意以下事项：

- View Portal 不提供虚拟打印功能或 USB 支持。
- 安装之后，系统不会为 View Portal 创建 Windows [Start （开始）] 菜单条目。

如果使用可执行文件安装 View Client，则该应用程序将提供虚拟打印功能和 USB 支持，并创建 [Start （开始）] 菜单条目。

注释 无论采用何种安装方式， View Portal 都不支持 USB 重定向。

安装 View Client

1 请在要安装客户端的系统中运行 View Client 可执行文件，其中 xxx 指文件的内部版本号：

```
VMware-viewclient-xxx.exe
```

2 显示 [VMware Installation （VMware 安装）] 向导时，请单击 **[Next （下一步）]**。

3 接受 VMware 许可条款并单击 **[Next （下一步）]**。

4 选择自定义的安装选项：

- 如果您不希望用户从桌面上访问本地连接的 USB 设备，可取消选择 **[USB Redirection （USB 重定向）]** 组件。
- 如果希望要求所有用户提供身份和凭据信息才能登录到 View Connection Server 并访问 View 桌面，可取消选择 **[Log in as current user （作为当前用户登录）]** 组件。

注释 Windows XP Home、 Windows Vista Home Basic、 Windows Vista Home Premium 和 Windows 2000 不支持 **[Log in as current user （作为当前用户登录）]** 功能。

5 如果选择了 **[Log in as current user（作为当前用户登录）]** 组件，您可以进一步配置用户通过 View Client 登录时的默认行为：

- 选择 **[Show in connection dialog（显示在 "连接" 对话框内）]**，可在 View Client 连接对话框中显示 **[Log in as current user （作为当前用户登录）]** 复选框。

  当选择了该复选框时，用户在登录客户端系统时提供的身份和凭据信息会传送到 View Connection Server 实例，最后传送到 View 桌面。
- 选择 **[Set default option to login as current user （设置默认选项，作为当前用户登录）]** 可默认选中 View Client 连接对话框中的 **[Log in as current user （作为当前用户登录）]** 复选框。

单击 **[Next （下一步）]**。

6 接受默认的目标文件夹或单击 **[Change （更改）]** 以使用其他的目标文件夹，然后单击 **[Next （下一步）]**。

7 （可选）输入客户端要连接的服务器的 IP 地址或 FQDN，然后单击 **[Next （下一步）]**。

8 配置 View Client 的快捷方式，然后单击 **[Next （下一步）]**。

9 安装完成后，要启动 View Client，请选中此复选框。

10 单击 **[Install （安装）] > [Finish （完成）]**。

启动 View Client

1 如果 View Client 在安装完成后没有自动启动，请双击桌面快捷方式或单击 **[Start （开始）]** > **[Programs （程序）]** > **[VMware]** > **[VMware View Client]**。

2 在 **[Connection Server （连接服务器）]** 下拉菜单中，输入 View Connection Server 的主机名或 IP 地址。

3 （可选）如果显示了 **[Log in as current user （作为当前用户登录）]** 复选框，您可以选中该复选框，以使用您在登录该系统时指定的凭据来登录 View Connection Server 和 View 桌面。

   如果未选择 **[Log in as current user （作为当前用户登录）]**，则需要多次提供凭据进行登录，才能访问 View 桌面。

   如果选择了 **[Log in as current user （作为当前用户登录）]**，并且有权登录 View Connection Server，则系统不会提示您输入步骤 5 中的登录凭据。

4 单击 **[Connect （连接）]**。

5 输入已获得授权的用户的凭据，选择域，然后单击 **[Login （登录）]**。

   如果输入的用户名格式为 `user@domain`，该用户名将因为带有 @ 符号而被视作用户主体名称 （User Principal Name， UPN）。因此域下拉菜单将会灰显。

6 从提供的列表中选择桌面，然后单击 **[Connect （连接）]**。

   View Client 将尝试连接到指定的桌面。

连接成功后，屏幕上将显示客户端窗口。

使用 View Portal 连接到桌面

1 打开 View Portal 所支持的浏览器，输入标准或副本 View Connection Server 或安全服务器实例的 URL。

2 输入已授权的用户的用户名和密码，然后从下拉菜单中选择正确的域并单击 **[Login （登录）]**。

3 当 [Access Status （访问状态）] 变为 [Ready （就绪）] 时，请单击要使用的桌面旁边的 **[Options （选项）]** > **[Connect （连接）]**。

View Client 策略

可通过策略来控制某些 View Client 功能。有关在全局级别、池级别或用户级别配置策略并将策略应用于 View Client 的信息，请参阅第 173 页上的 “客户端策略”。

通过 Internet 执行客户端连接

若用户要访问虚拟桌面，则其客户端系统必须能够解析指定的 View Connection Server 主机名或 IP 地址。最初，在默认情况下只能通过安全加密链路客户端来连接 View Connection Server ；这些安全加密链路客户端与服务器位于同一网络中，因而能够找到所请求的服务器。

许多组织都要求用户通过以下任何一种方式从外部进行连接：使用可全局解析的域名、子域名或 IP 地址；或者将特定端口重新分配给现有地址，以便将客户端的请求传送到适当位置 （通常是安全服务器）。例如：

- `https://view-example.com:443`
- `https://view.example.com:443`
- `https://example.com:1234`

不过，还必须在 View Connection Server 中进行其他配置，才能正常使用这些地址。

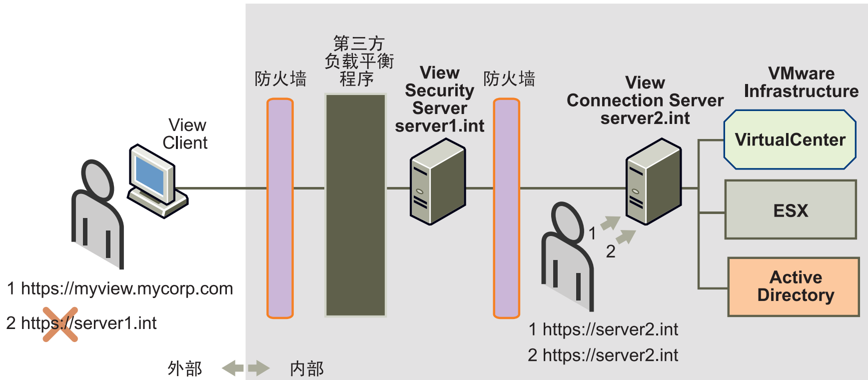
设置 View Connection Server 的外部 URL

当您使用 Microsoft RDP 作为显示协议时， View Client 会尝试在自身与 View Connection Server 之间创建两个单独的 TCP 连接。第一个连接用来处理用户操作，例如身份验证、桌面选择等。第二个连接在登录后进行实例化，并成为传输 RDP 数据的安全加密链路。

第一个连接是通过用户在客户端中输入的 URL 或 IP 地址创建的。如果在网络环境中正确配置了防火墙和负载平衡组件，则该请求能够到达服务器。完成身份验证后，系统会将 View Connection Server 的 FQDN 返回到客户端。

系统将使用 FQDN 尝试执行第二个连接 （默认情况下用 SSL 加密的安全加密链路连接）。但是，如果外部 View Client 无法解析该 FQDN，连接将失败。图 5-1 显示了外部及内部客户端与服务器交互操作的顺序示例。

图 5-1. 外部客户端连接



此时，将 View Connection Server 配置为返回外部 URL 而不是用于第二连接通道的 FQDN，可解决连接失败的情况。

对于不同类型的服务器来说，设置外部 URL 的过程有所不同。对于标准或副本服务器，您可以从 View Administrator 中设置 URL。对于安全服务器而言，您必须创建或编辑一个包含入站连接详细信息的属性文件，并将其保存在安全服务器安装路径下的目录中。

警告 对于安全服务器而言，如果您要在 View 环境中使用消息安全模式，则必须使用第 95 页上的 "从 [Configuration （配置）] 视图中生成安全服务器的 config.properties 文件"中介绍的方法，此操作过程创建的配置文件包含对这种全局配置至关重要的信息。

在标准服务器或副本服务器中设置外部 URL

1 在 View Administrator 中，单击 **[Configuration （配置）]** 按钮。

2 在 [View Servers （View 服务器）] 下，选择 [View Connection Server] 条目并单击 **[Edit （编辑）]**。

3 在 **[External URL （外部 URL）]** 字段中输入 URL。该名称必须包含协议、地址和端口号。例如：

```
https://view.example.com:443
```

单击 **[OK （确定）]**。

安全服务器的外部 URL

无法从 View Administrator 中定义安全服务器的外部 URL。您可以使用 View Administrator 生成包含可外部解析的安全服务器名称、端口号和协议的配置文件。此文件会放在安全服务器上。

从 [Configuration （配置）] 视图中生成安全服务器的 config.properties 文件

1 在与安全服务器关联的标准或副本服务器的 View Administrator 中，单击 **[Configuration （配置）]** 按钮。单击左侧窗格中的 **[Servers （服务器）]** 条目。

2 在 [Security Servers （安全服务器）] 下，单击 **[Add （添加）]**。随即显示 [Add Security Server （添加安全服务器）] 窗口。

3 在 **[Server Name （服务器名称）]** 字段中，输入安全服务器的 FQDN。

4 在 **[External URL （外部 URL）]** 字段中输入外部 URL。该名称必须包含协议、地址和端口号。例如：

```
https://view.example.com:443
```

单击 **[OK （确定）]**。安全服务器将添加到 [Configuration （配置）] 视图的 [Security Servers （安全服务器）] 列表中。

5 选择该安全服务器条目，并单击 **[Create Configuration File （创建配置文件）]**。浏览器将下载配置文件。

6 在便于访问的位置将此文件另存为 `config.properties` 文件，然后将其复制到安全服务器中的以下位置：

```
C:\Program Files\VMware\VMware View\Server\sslgateway\conf
```

注释 在安全服务器中，必须重新启动 VMware View Security Server 服务，上述更改才能生效。

创建 SSL 服务器证书

安全套接字层 （Secure Sockets Layer， SSL）证书是一个通过密码密封的数据对象，它包含服务器标识、服务器公用加密密钥，以及证书颁发者的数字签名。证书具有两大用途：

- 它们可向客户端提供经过身份验证的证明，即客户端访问的网站归安装该证书的公司或个人所有。
- 它们包含客户端用来与服务器建立加密连接的公用密钥。

默认情况下，在 View Connection Server 中，当客户端访问安全页面（例如，View Administrator）时，将向其呈现应用程序提供的自行签署式证书。通过阅读服务器证书，用户可确定该服务器是否为受信任的源，然后决定接受（或拒绝）该连接。

证书可由证书颁发机构 (Certificate Authority, CA) 签发，该机构是确保证书及其创建者身份的受信任的第三方。

要创建您自己的 View Connection Server 证书，请执行以下操作之一：

- 您可使用 View Connection Server 附带的 Java Runtime Environment (JRE) 实例提供的 `keytool` 实用程序，为系统创建自行签署式证书。自行签署式证书是指由用户生成、且未通过任何受信任的 CA 正式注册、因而无法保证身份的证书。
- 创建证书，并向 CA 发送包含证书详细信息的证书签发请求（Certificate Signing Request，CSR）。在对提出申请的公司或个人进行检查之后，CA 会签发该请求并使用私用密钥进行加密。有效证书将返回并插入到 View Connection Server 中的密钥存储区。

注释 在准备好创建自己的证书并使其通过 CA 签发之前，强烈建议您继续使用 View Connection Server 提供的默认证书。

连接到 View Connection Server 的客户端将与证书一起显示。如果证书为自行签署式证书但已为用户接受、或已由客户端浏览器信任的 CA 签发，则客户端会使用证书内包含的公用密钥将发送到 View Connection Server 的数据加密。通常，CA 自身的证书嵌入在浏览器中，或位于客户端可访问的受信任数据库中。

注释 只有接收客户端直接连接的标准服务器、副本服务器或安全服务器，才要求使用证书。如果您将安全服务器作为面向客户端的系统，则只有该服务器要求使用证书。

接受证书后，客户端会通过发送密钥（由服务器公用密钥加密）来做出响应。此密钥用于加密客户端和 View Connection Server 实例或安全服务器之间的通信量。

默认情况下，View Connection Server 包含自行签署式 SSL 证书，客户端可在连接时使用该证书创建安全会话。尽管该证书不受客户端信任，且不具备正确的服务名称，但它确实允许连接。

您可以将 View 提供的默认证书替换为针对该服务正确定义的证书。如果证书由受信任的 CA 签发，则系统不会向用户显示要求验证证书的消息，且瘦客户端设备可以执行连接，无需进行其他配置。

要创建和安装您自己的证书，必须先将 Java `keytool` 实用程序添加到命令路径中，以便使用命令提示符从任意位置执行该程序。完成此操作后，您可以使用 `keytool` 实用程序创建自行签署式 SSL 证书。

要获得受信任的第三方签发的验证证书，必须先向 CA 提交证书签发请求 （Certificate Signing Request， CSR）。从 CA 收到受信任证书之后，您可以将其导入到 View Connection Server 的密钥存储区，然后配置 View Connection Server 以使用该证书。

注释 您可能已拥有要与 View Connection Server 结合使用的 SSL 证书。有关如何执行此操作的详细信息，请参阅第 100 页上的 "使用现有 SSL 证书"。

创建 SSL 证书

确定要与证书绑定的名称时，您应慎重考虑。证书可将服务名称与加密密钥对绑定在一起，通过执行此操作，可取得服务和密钥的所有权。

证书签发之后，客户端将信任该服务器 （及其加密密钥），这是因为 CA 可独立地确定声明所有权的单位已请求该密钥。

证书最重要的部分是公用名称 （Common Name, CN）属性。使用客户端计算机用来连接到 View Connection Server 的 FQDN。在单台服务器环境中，该名称通常是指服务器名称。如果使用负载平衡，则请使用负载平衡器名称。

在系统路径中添加 Java keytool

1 请同时按 Windows 键和 Break 键，以显示 Windows [System Properties （系统属性）] 对话框。

2 在 **[Advanced （高级）]** 选项卡下，请单击 **[Environment Variables （环境变量）]**。

3 在系统变量组中，请选择 **[PATH （路径）]**，然后单击 **[Edit （编辑）]**。

4 在 **[Variable value （变量值）]** 字段中，将以下路径添加到 JRE 安装目录中：

```
%ProgramFiles%\VMware\VMware View\Server\jre\bin
```

请确保使用分号 （**;**）将此条目与字段中显示的任何其他条目相分隔。

5 依次单击 **[OK （确定）]** > **[OK （确定）]** > **[OK （确定）]**，以关闭 Windows [System Properties （系统属性）] 对话框。

创建自行签署式 SSL 证书

1 通过命令提示符，输入以下内容：

```
keytool -genkey -keyalg "RSA" -keystore keys.p12 -storetype pkcs12
-validity 360
```

2 系统将提示您输入密钥存储区的密码，然后提供您自己和单位的信息。当系统要求您输入名称时，请输入要保护的 View Connection Server 实例的 FQDN。

3 请输入部门、单位、地址、省 / 市以及国家 / 地区。最后一项必须采用两个字母的国家 / 地区代码格式。

4 屏幕中将显示您已输入的数据摘要，并询问您是否继续。如果所有详细信息均正确无误，请输入 `yes` （是）。

5 系统将提示您输入密码，这是该证书 （与存储在同一密钥存储区文件中的任何其他证书相对）的专用密码。系统会在当前目录中创建 `keys.p12` 文件。

建议在将证书导入 `keys.p12` 文件后对该文件进行备份，以便您以后重新构建服务器配置。

验证 SSL 证书

尽管自行签署式证书足以保证服务器和客户端之间的数据加密，但它并不提供有关 View Connection Server 位置、或负责管理证书的公司实体所处位置的任何可靠信息。

客户端必须能够确定所接收数据的来源和完整性，这至关重要。因此，建议您为站点获取通过 CA 身份验证的证书。

创建证书签发请求 (CSR)

通过命令提示符输入以下内容，其中 `<secret>` 是密钥存储区密码：

```
keytool -certreq -keyalg "RSA" -file certificate.csr -keystore keys.p12
-storetype pkcs12 -storepass <secret>
```

系统会在同一位置创建 `certificate.csr` 文件。此文件内容应类似于以下示例 （比该示例略长）：

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBuDCCASECAQAweDELMAkGA1UEBhMCR0IxEDAOBgNV
BAgTB1Vua25vd24xEDAOBgNVBAcTB1Vua25vd24xFDAS
BgNVBAoTC1ZNd2FyZSBJbmMuMRMwEQYDVQQLEwp2bXdh
XU8/2jEUL5DocLDLnygsUD2g7cUMYdz/HeECAwEAAaAA
AeHnsPs7a1Q0JH6OZvdU
-----END NEW CERTIFICATE REQUEST-----
```

提交 CSR 并导入证书

1 请根据注册过程将 CSR 文件发送到证书颁发机构，并请求 PKCS#7 格式的证书。在此过程中，您可能需要提供身份证明、域所有权证明等。

出于测试目的，许多证书颁发机构还提供基于不受信任的根的临时性免费 SSL 证书：

Thawte：https://www.thawte.com/cgi/server/try.exe

VeriSign：http://verisign.com/ssl/buy-ssl-certificates/free-ssl-certificate-trial

GlobalSign：http://globalsign.com/free-ssl-certificate/free-ssl.htm

一些 CA 只提供 PKCS#12 格式的证书。要下载此类型的证书，则必须参阅第 100 页上的 “将 PKCS#12 证书转换为 PKCS#7 格式”，以了解有关如何将证书文件转换为 PKCS#7 格式的信息，然后再继续。

2 如果您已经从 CA 收到临时或完整的证书，请将文件内容复制到文本编辑器，并将其另存为 `certificate.p7`。此文件的内容将类似于以下示例 （比该示例略长）：

```
-----BEGIN PKCS7-----
MIIF+AYJKoZIhvcNAQcCoIIF6TCCBeUCAQExADALBgk
LDCCApWgAwIBAgIQTpY7DsV1n1HeMGgMjMR2PzANBgk
i7coVx71/lCBOlFmx66NyKlZK5mObgvd2dlnsAP+nnS
EhCsdpikSpbtdo18jUubV6z1kQ71CrRQtbi/WtdqxQE
-----END PKCS7-----
```

3 通过命令提示符输入以下内容，其中 `<secret>` 是密钥存储区密码：

```
keytool -import -keystore keys.p12 -storetype pkcs12 -storepass <secret>
-keyalg "RSA" -trustcacerts -file certificate.p7
```

如果您使用临时证书，则将看到以下消息：

```
... is not trusted. Install reply anyway?
```

由于指定给您的根证书是测试证书，且不用于生产环境，因此它不受 Java 信任，结果导致生成上述消息。

配置 View Connection Server 以使用新证书

1 请将新证书文件放置在 View Connection Server 的标准、副本或安全服务器实例的以下位置：

```
C:\Program Files\VMware\VMware View\Server\sslgateway\conf
```

2 在每台服务器中创建或编辑以下文件：

```
C:\Program Files\VMware\VMware View\Server\sslgateway\conf\
locked.properties
```

3 添加以下属性：

```
keyfile=keys.p12
keypass=<secret>
```

这些值需要更改成与您在先前步骤中创建的内容匹配。

4 重新启动 View Connection Server 服务。假定您的环境已配置为使用 SSL，则 View Connection Server 日志中将出现类似于以下内容的消息：

```
13:57:40,676 INFO  <Thread-1> [NetHandler] Using SSL certificate store:
keys.p12 with password of 6 characters
```

上述消息指出配置已生效。

将 PKCS#12 证书转换为 PKCS#7 格式

1 创建一个 PKCS#12 证书，并在导出该文件时选择 Tomcat 作为 Web 服务器类型。

2 在 Windows Explorer 中打开证书文件。

3 单击 **[Details （详细信息）]** > **[Copy to File （复制到文件）]** > **[PKCS7]**。

4 选择 **[Include Details of Certificate （包含证书详细信息）]**。

5 以 `.P7` 为扩展名保存该文件。

6 将此证书添加到密钥存储区，如第 98 页上的 "提交 CSR 并导入证书" 中所述。

使用现有 SSL 证书

您的单位可能已拥有要与 View Connection Server 结合使用的有效 （经过 CA 签发） SSL 证书。要使用 SSL 证书，您必须使用该证书及其附带的私用密钥。

从 Microsoft IIS Server 中导出

要使用现有的 Microsoft IIS SSL 服务器证书，必须先将其从装有网站 （使用该证书） 的 IIS 应用程序服务器中导出。 Windows 提供了许多可视工具，帮助您导出证书。

从 IIS 应用程序中导出 SSL 服务器证书

1 在 IIS 应用程序服务器主机系统中，单击 **[Start （开始）]** > **[Administrative Tools （管理工具）]** > **[Internet Information Services (IIS) Manager （Internet 信息服务 (IIS) 管理器）]**。随即显示 [Internet Information Services Manager （Internet 信息服务管理器）]。

2 从左侧窗格的树状小部件中，展开 [Local computer （本地计算机）] 条目，然后单击 [Web Sites （网站）] 以查看服务器所装载的网站列表。

3 在右侧窗格中，右键单击包含要导出的 SSL 证书的网站条目，然后从上下文菜单中选择 **[Properties （属性）]**。随即显示 [Web site properties （网站属性）] 窗口。

4 选择 **[Directory Security （目录安全性）]** 选项卡。在 [Secure communications （安全通信）] 下，单击 **[Server Certificate （服务器证书）]**。随即显示 [Web Server Certificate （Web 服务器证书）] 向导。单击 **[Next （下一步）]**。

5 选择 **[Export the current certificate to a .pfx file （将当前证书导出为 .pfx 文件）]**。单击 **[Next （下一步）]**。

6 指定要导出的文件的文件名。单击 **[Next （下一步）]**。

7 输入并确认用来加密导出信息的密码。单击 **[Next （下一步）]**。

8 屏幕中将显示您要导出的证书摘要。确保这些摘要信息正确无误 （且您已选择正确的证书）， 然后单击 **[Next （下一步）]** > **[Finish （完成）]**。

证书将导出到指定位置。现在，您必须执行第 99 页上的 “配置 View Connection Server 以使用新证书”中所述的步骤。请确保 `locked.properties` 文件中的 `keypass` 条目与导出证书时使用的密码一致。

智能卡身份验证

有些组织要求职员通过多个阶段的身份验证，才能连接到系统。 View 会针对客户端会话提供智能卡身份验证，从而可支持高安全性的环境。

智能卡身份验证可向 View Connection Server 展示一整套受信任的客户端凭据 （用户证书）。用户证书是指一整套加密的身份验证凭据，其中包括颁发该证书的受信任根证书颁发机构 （CA）的数字签名。

用户证书存储在智能卡中，仅当用户通过输入个人标识号 （Personal Identification Number, PIN）验证所有权后，才能检索该证书并将其传输至服务器。然后，系统将使用公用密钥对证书进行身份验证，以验证其中包含的数字签名；预期的数字签名包含在 View Connection Server 内存储的受信任 CA 证书中。

下面的部分将介绍如何在 View Connection Server 中配置并启动此功能。

注释 智能卡身份验证仅受 View Client 支持。 View Administrator、 View Portal 或通过 View Client with Offline Desktop 访问的脱机桌面实例均不支持此功能。

智能卡硬件

每个使用智能卡身份验证的客户端系统都将要求安装 View Client 和 Windows 兼容的智能卡读卡器。

为了识别并使用智能卡硬件，必须在客户端系统和远程桌面中安装与产品特定相关的应用程序驱动程序。根据供应商的不同，智能卡的配置文件可能会有所不同。有关如何执行此操作的更多信息，请参阅智能卡读卡器附带的文档。

获得根证书

您必须从针对用户提供的智能卡签发证书的 CA 处获得根证书。您可从以下一种源中获得根证书：

- 运行 Microsoft 证书服务的 Microsoft IIS Server。安装 Microsoft IIS、颁发证书并在单位范围内分发证书的过程已超出本指南范围，在此概不赘述。要了解上述任务的更多信息，请参阅下面的 Web 资源：
  - 如何在 Windows Server 2003 中安装 IIS：
    http://technet.microsoft.com/library/aa998483.aspx
  - 管理 Microsoft 证书服务：
    http://technet.microsoft.com/library/bb727098.aspx
- 受信任第三方 CA 签发的公用根证书。如果已预先存在智能卡基础架构，且已制定标准方式来分发智能卡和进行身份验证（例如，政府和军事机构），则您可能更倾向于从这种来源获得根证书。

确定要使用的正确证书之后，签发链将列出一系列签发机构。通常，最好选择用户证书上方紧邻的中间机构。请检查该机构未用来签发智能卡中的其他证书。

从用户证书中导出根证书

如果您没有 CA 的根证书，但拥有 CA 签发的用户证书，或包含一种证书的智能卡，则可在根证书受系统信任的情况下根据这些信息导出根证书。

注释 如果您已拥有包含用户证书的智能卡，请将该智能卡插入读卡器。许多情况下，执行此操作会将用户证书自动添加至个人存储区。如果未添加，则您必须使用读卡器附带的软件，将用户证书导出至某个文件。稍后，您可在以下步骤中将该文件导入到 Internet Explorer。

从用户证书中导出根证书

1 启动 **[Internet Explorer]**，并单击 **[Tools（工具）]** > **[Internet Options（Internet 选项）]**。

2 在 **[Content （内容）]** 选项卡下，单击 **[Certificates （证书）]**。

3 在 **[Personal （个人信息）]** 选项卡下，选择要使用的证书并单击 **[View （查看）]**。

   注释 如果列表中未显示用户证书，则必须先单击 **[Import （导入）]** 按钮，以手动导入用户证书。导入证书之后，从列表中选中该证书并单击 **[View （查看）]**。

   ---

4 在 **[Certification Path （证书路径）]** 选项卡下，选择树状视图顶部的证书并单击 **[View Certificate （查看证书）]**。

5 在 **[Details （详细信息）]** 选项卡下，单击 **[Copy to File （复制到文件）]**。随即显示 [Certificate Export Wizard （证书导出向导）]。

6 单击 **[Next （下一步）]** > **[Next （下一步）]**，输入要导出的文件名称和位置。

7 单击 **[Next （下一步）]**。文件将在指定位置另存为根证书。

信任层次结构

用户证书可作为信任层次结构的一部分签发，即签发的证书本身可能由另一较高级别的证书签发。

尽管允许使用层次结构任何级别签发的任何证书，但最好使用父证书 （即，实际签发了用户证书的证书）作为根证书。

向 Active Directory 中受信任的根添加根证书

本部分介绍如何将第三方根 CA 证书导入至 Active Directory 和 Enterprise NTAuth 存储中。

仅当您使用第三方 CA 颁发智能卡徽标或域控制器证书时，才需执行以下步骤；如果使用 Windows 域控制器作为根 CA，则无需执行。

向 Active Directory 组策略对象中受信任的根添加第三方根 CA

1 单击 **[Start （开始）]** > **[All Programs （所有程序）]** > **[Administrative Tools （管理工具）]** > **[Active Directory Users and Computers （Active Directory 用户和计算机）]**。

2 在左侧窗格中，找到已应用您要编辑的策略的域。

3 右键单击该域，然后单击 **[Properties （属性）]**。

4 在 [Group Policy （组策略）] 选项卡下，单击 **[Default Domain Policy Group Policy （默认域策略的组策略）]** 对象，然后单击 **[Edit （编辑）]**。随即显示一个新窗口。

5 在左侧窗格中，展开 **[Computer Configuration （计算机配置）]** > **[Windows Settings （Windows 设置）]** > **[Security Settings （安全设置）]** > **[Public Key Policy （公用密钥策略）]**。

6 右键单击 **[Trusted Root Certification Authorities（受信任的根证书颁发机构）]**，然后选择 **[Import （导入）]**。

7 请按照向导中的说明导入证书。单击 **[OK （确定）]**。

8 请关闭 [Group Policy （组策略）] 窗口。

通过将证书添加到受信任的根证书列表，您可以确保域中的所有系统在受信任的根存储区中均拥有证书副本。

向 Active Directory 中的 NTAuth 存储区添加第三方根证书 CA

通过 Active Directory 命令行提示符输入以下内容：

```
certutil -dspublish -f <certificate> NTAuthCA
```

在此命令中， `<certificate>` 是第三方根 CA 证书的路径。

通过将证书发布到 Enterprise NTAuth 存储区，您可以确认 CA 是否是颁发此类证书的受信任颁发机构。

创建信任存储区

信任存储区是指 View 在确定信任哪些客户端时使用的密钥存储区。为了让 View Connection Server 对智能卡用户进行身份验证并将他们连接到桌面，所有受信任用户的根证书必须先添加到服务器的信任存储区。

您可使用 View Connection Server 附带的 Java Runtime Environment (JRE) 实例提供的 `keytool` 实用程序创建信任存储区。

在命令路径中添加 JRE 实用程序

1 请同时按 Windows 键和 Break 键，以显示 Windows [System Properties （系统属性）] 对话框。

2 在 **[Advanced （高级）]** 选项卡下，请单击 **[Environment Variables （环境变量）]**。

3 在系统变量组中，请选择 **[PATH （路径）]**，然后单击 **[Edit （编辑）]**。

4 在 **[Variable value （变量值）]** 字段中，将以下路径添加到 JRE 安装目录中：

```
%ProgramFiles%\VMware\VMware View\Server\jre\bin
```

请确保使用分号 （**;**）将此条目与字段中显示的任何其他条目相分隔。

5 依次单击 **[OK （确定）]** > **[OK （确定）]** > **[OK （确定）]**，以关闭 Windows [System Properties （系统属性）] 对话框。

使用 keytool 创建信任存储区

通过命令提示符，输入以下内容：

```
keytool -import -alias <别名> -file <证书名称>
    -keystore <信任存储区文件名>
```

在此命令中，<别名>是指信任存储区中新实体条目（在此情况下，指的是要导入的证书）的唯一名称（不区分大小写）；<证书名称>是指您先前获得或导出的根 CA 证书的名称，而<信任存储区文件名>是指信任存储区输出文件的名称。

注释 系统可能会要求您为密钥存储区创建密码；这并非执行后续步骤的必要条件，但如果将来要在信任存储区添加其他证书，则应记住所创建的密码。

启动服务器中的智能卡身份验证

尽管各种 View Connection Server 均支持智能卡身份验证，但建议仅将安全服务器配置为允许智能卡访问。如果向标准或副本服务器添加智能卡支持，则每次连接到这些系统中的 View Administrator 时，系统将提示您选择证书。

注释 如果并非所有用户都需要使用智能卡进行身份验证，则建议您专门为客户端智能卡身份验证配置新的（或其他）安全服务器。

向 View Connection Server 添加智能卡身份验证

1 将先前创建的信任存储区文件（`<truststore_filename>`）复制到 View Connection Server 中的以下位置：

```
C:\Program Files\VMware\VMware View\Server\sslgateway\conf\
```

2 请创建一个包含以下条目的名为 `locked.properties` 的文本文件：

```
trustKeyfile=<truststore filename>
trustStoretype=JKS
useCertAuth=true
```

`trustKeyfile` 的值必须与<信任存储区文件名>的值一致。

必须重新启动 View Connection Server 服务，上述更改才能生效。

注释 配置标准或副本 View Connection Server 之后，系统将在您登录到该服务器中的 View Portal 或 View Administrator 时提示您选择证书。

验证智能卡身份验证配置

当您首次设置智能卡身份验证，或智能卡身份验证无法正常工作时，应检查智能卡的身份验证配置。

验证智能卡的身份验证配置

- 确认每个客户端系统都配置了 View Client、智能卡中间件、带有有效证书的智能卡和读卡器。

  有关配置智能卡软件和硬件的信息，请参见您的智能卡供应商提供的文档。

- 在每个客户端系统上，选择 **[Start（开始）]** > **[Settings（设置）]** > **[Control Panel（控制面板）]** > **[Internet Options （Internet 选项）]** > **[Content （内容）]** > **[Certificates （证书）]** > **[Personal （个人）]**，查看证书能否用于智能卡身份验证。

  用户将智能卡插入读卡器后， Windows 会将其中的证书复制到用户计算机上，以便 View Client 使用这些证书。

- 在 View Connection Server 或安全服务器主机的 `locked.properties` 文件中，检查 **[useCertAuth]** 的属性是否被设置为 `[true]` 且拼写正确。

  `[locked.properties]` 文件位于以下文件夹内：
  < 安装目录 >`\VMware\VMware View\Server\sslgateway\conf`

- 如果您在 View Connection Server 实例上配置了智能卡身份验证，请在 View Administrator 中检查智能卡的身份验证设置。

  a 在 View Server 下，选择 [View Connection Server] 实例并单击 **[Edit（编辑）]**。

  b 检查 **[Smart card authentication （智能卡身份验证）]** 是否被设置为 **[Optional （可选）]** 或 **[Required （必需）]**。

  必须重新启动 View Connection Server 服务，对智能卡设置所做的更改才能生效。

- 如果智能卡用户所在的域和颁发根证书的域不同，请检查用户的用户主体名称（User Principal Name， UPN）是否被设置为受信证书颁发机构 （Certificate Authority， CA）根证书内包含的主题备用名称 （Subject Alternative Name，SAN）。

  a 在您的 Active Directory 服务器上，选择 **[Start （开始）]** > **[Administrative Tools （管理工具）]** > **[Active Directory Users and Computers （Active Directory 用户和计算机）]**。

  b 右键单击 **[Users （用户）]** 文件夹中的用户，然后选择 **[Properties （属性）]**。

  UPN 出现在 [Account（帐户）] 选项卡的 [User Logon Name（用户登录名）] 字段内。

  查看 View Connection Server 或安全服务器主机上 < 驱动器 >`:/Documents and Settings/All Users/Application Data/VMware/VDM/logs` 目录下的日志文件，以找到指出已启用智能卡身份验证的消息。

配置标准服务器或副本服务器

已配置使用智能卡身份验证的安全服务器将自动要求用户使用登录过程中的智能卡和 PIN 进行身份验证。您可对标准和副本服务器进行配置，使其支持多种不同的智能卡身份验证方案。

在标准或副本服务器中设置智能卡身份验证

1 在 View Administrator 中，单击 **[Configuration （配置）]** 按钮。

2 在 [View Servers （View 服务器）] 下，选择 [View Connection Server] 条目并单击 **[Edit （编辑）]**。

3 从 **[Smart card authentication （智能卡身份验证）]** 下拉菜单中，选择以下选项之一：

- **[Not allowed （不允许）]**：表示已禁用智能卡身份验证。
- **[Optional （可选）]**：表示用户可以使用智能卡身份验证进行连接，但亦允许使用密码身份验证。如果无法使用智能卡身份验证进行身份验证，则可使用密码身份验证。
- **[Required （必需）]**：表示用户仅可使用智能卡身份验证进行连接。

  需要进行智能卡身份验证时，如果用户在连接 View Connection Server 实例时选中了 **[Log in as current user（作为当前用户登录）]** 复选框，身份验证将会失败。这些用户必须在登录 View 桌面时重新用智能卡和 PIN 进行身份验证。

4 配置智能卡移除策略。

注释 当智能卡身份验证被设置为 **[Not Allowed （不允许）]** 时，您无法配置智能卡移除策略。

- 如果希望在用户移除智能卡时与 View Connection Server 实例断开连接，请选择 **[Disconnect user sessions on smart card removal （移除智能卡时断开用户会话）]** 复选框。用户必须重新进行身份验证，才能访问其 View 桌面。
- 如果希望在用户移除智能卡时与 View Connection Server 实例保持连接，请取消选择 **[Disconnect user sessions on smart card removal （移除智能卡时断开用户会话）]** 复选框。用户无需重新进行身份验证即可发起新的 View 桌面会话。

智能卡移除策略不适用于在选择了 **[Log on as current user（作为当前用户登录）]** 复选框的情况下连接 View Connection Server 实例的用户，即使他们使用智能卡来登录其客户端系统，也无法使用此策略。

5 单击 **[OK （确定）]**。

6 重新启动 View Connection Server 服务。

注释 智能卡身份验证仅可替换 Windows 密码身份验证。如果已启动 SecurID，则仍要求用户采用此机制进行身份验证。

配置用户配置文件

用户主体名称 （User Principal Name, UPN）是指识别用户帐户所在域的帐户名和域名。 UPN 的常见格式为：`user@domain`。对于使用智能卡身份验证进行连接的用户而言，其 Active Directory 中的帐户必须具有与其 `userPrincipalName` 属性相关的有效 UPN。

对于要求使用智能卡身份验证的每位用户而言，必须将其 UPN 设为受信任 CA 根证书内包含的主题备用名称 （Subject Alternative Name, SAN）。您可以通过查看第 102 页上的 "从用户证书中导出根证书" 中介绍的证书属性找到此信息。

注释 仅当该证书由其他域签发，而不是用户当前域签发时，您才需要提供此信息。从用户当前域中的服务器导出证书的特征是：用户的 UPN 与根证书 SAN 彼此关联。

将此信息添加到 Active Directory 的最直接方法是使用 ADSI Edit 实用程序 （随 Windows 支持工具软件集提供）。如果您的 Active Directory 服务器中没有该实用程序，您可以从以下位置下载并安装 Windows 支持工具：

http://www.microsoft.com/downloads/details.aspx?FamilyID=96a35011-fd83-419d-939b-9a772ea2df90

在 Active Directory 中将 UPN 设置为 SAN

1 在 Active Directory 服务器上，单击 **[Start （开始）]** > **[All Programs （所有程序）]** > **[Windows Support Tools （Windows 支持工具）]**，在支持工具目录位置打开命令提示符。

2 输入 `adsiedit.msc`，以启动 ADSI Edit 应用程序。

3 在左侧窗格中，依次展开要编辑的用户所在的域和 **CN=Users**。

4 右键单击该用户，然后单击 **[Properties （属性）]**。随即显示用户的属性编辑窗口。

5 从列表中，双击 `userPrincipalName` 条目。在提供的字段中，输入受信任 CA 证书的 SAN 值。

6 单击 **[OK （确定）]** > **[OK （确定）]**，关闭 ADSI Edit。

RSA SecurID 身份验证

View 支持将 RSA SecurID 用作额外的用户身份验证方法。除了在使用 Active Directory 凭据时提供身份验证之外， RSA SecurID 还可在用户访问虚拟桌面时提供功能强大的双因素身份验证。

如果使用 RSA SecurID，则必须先通过编辑 View Connection Server 设置进行启动。在一台或多台服务器中安装 RSA SecurID 软件之后，您可以在 View Administrator 用户界面中编辑 RSA 设置。

启动或编辑 RSA SecurID

1 在 View Administrator 中，单击 **[Configuration （配置）]** 按钮。

2 在 [View Servers （View 服务器）] 下，选择 [View Connection Server] 条目并单击 **[Edit （编辑）]**。

3 在 [RSA SecurID 2-Factor Authentication （RSA SecurID 双因素身份验证）] 标题下，配置所需的 RSA 设置：

- **[Enable （启用）]**：为访问虚拟桌面的最终用户启用 RSA SecurID 身份验证。
- **[Enforce SecurID and Windows user name matching（强制匹配 SecurID 和 Windows 用户名）]**：SecurID 根据 Active Directory 的用户名来检查用户名，并拒绝访问不匹配的条目。
- **[Clear node secret （清除节点秘密）]**：请参阅 View Agent 中的节点秘密。请参阅 "重置节点秘密。"

有关此设置的更多信息，请参阅 RSA Authentication Manager 用户文档。

4 在 **[Upload RSA authentication agent configuration file (sdconf.rec)（上传 RSA 身份验证代理配置文件 (sdconf.rec)）]** 字段中，输入 `sdconf.rec` 文件的位置或单击 **[Browse （浏览）]** 搜索该文件。有关 `sdconf.rec` 文件的更多信息，请参阅 RSA Authentication Manager 用户文档。单击 **[OK （确定）]**。

重置节点秘密

如果通过 RSA SecurID 进行验证的 View Client 连接显示 `[Access Denied` （拒绝访问）] 且 RSA Authentication Manager 登录监视器显示 `[Node verification Failed` （验证节点失败）]，则请清除 View Connection Server 中的节点秘密，然后进行以下操作：

1 运行 **[RSA Authentication Manager Host Mode（RSA Authentication Manager 主机模式）]**。

2 选择 **[Agent Host menu （代理主机菜单）]** > **[Edit Agent Host （编辑代理主机）]**。

3 从列表中选择 **[View Connection Server]**，然后选择 **[OK （确定）]**。

4 取消选择 **[Node Secret Created （已创建节点秘密）]** 并单击 **[OK （确定）]**。

注释 每当您进行编辑时，将默认选中 **[Node Secret Created （已创建节点秘密）]**。

View Client 命令行选项

View Client 提供了许多启动选项，可在启动应用程序时通过命令提示符调用它们。选项的前面均带有连字符 （-） 或正斜线 （/），选项不区分大小写，且可以缩写成唯一最短格式。例如，要显示命令的完整列表，请输入以下内容：

```
"C:\Program Files\VMware\VMware View\Client\bin\wswc" /?
```

要在完全脚本化的模式 （提供了所有连接、用户和桌面标准）中启动 View Client，请输入以下内容：

```
"C:\Program Files\VMware\VMware View\Client\bin\wswc" -serverURL <服务器>
-userName <用户名> -password <密码> -domainName <域> -desktopName <桌面>
```

表 5-1 中列出了启动 View Client 时可以使用的命令行选项。

表 5-1. View Client 命令行选项

属性	描述
`file <xxx>`	带有其他命令行参数的文本文件。请参阅第 112 页上的 "View Client 配置文件"。
`nonInteractive`	用来在完全脚本化的启动过程中禁止显示错误消息框。
`languageId <xxx>`	为 View Client 中的不同语言提供本地化支持。如果有可用的资源库，您可以指定要使用的 Windows 语言 ID。 对于中国简体中文，请输入 `0x804`
`desktopLayout <xxx>`	用户登录 View 桌面时看到的 View Client 窗口布局。 布局选项包括： ■ `fullScreen` （全屏） ■ `multimonitor` （多显示器） ■ `windowLarge` （大窗口） ■ `windowSmall` （小窗口） 此属性要求提供 `desktopName` 属性。
`desktopName <xxx>`	选定桌面列表对话框中的桌面名称。 **注释：** 这是您在选定桌面列表对话框中看到的名称。

表 5-1. View Client 命令行选项 （续）

属性	描述
desktopProtocol <xxx>	选定桌面列表对话框中的显示协议名称。 **注释：**这是您在选定桌面列表对话框中看到的名称。
logInAsCurrentUser <xxx>	与在桌面对话框中选中 **[Log in as current user: <xxx> （作为当前用户登录：<xxx>）]** 后的行为相同。 如果指定了该属性，用户在登录客户端系统时提供的身份和凭据信息会传送到 View Connection Server 实例，最后传送到 View 桌面。
serverURL <xxx>	View Connection Server 的 URL。
userName <xxx>	View Client 在登录过程中使用的用户名。
password <xxx>	View Client 在登录过程中使用的密码。
domainName <xxx>	View Client 在登录过程中使用的域名。
rollback	（仅适用于 Offline Desktop）解除锁定已检出的桌面联机版本，并放弃脱机会话。 此属性要求提供 desktopName 属性。
checkout	（仅适用于 Offline Desktop）检出指定的桌面，锁定 Server 端桌面。 此属性要求提供 desktopName 属性。
checkin	（仅适用于 Offline Desktop）检入指定的桌面，解除锁定 Server 端桌面。 此属性要求提供 desktopName 属性。
staycheckedout	（仅适用于 Offline Desktop）将已检出桌面的数据备份到服务器，但保持脱机桌面的检出状态。 此属性要求提供 desktopName 属性。
offlineDirectory <xxx>	（仅适用于 Offline Desktop）指定用来下载新脱机桌面的本地目录路径。 此属性要求提供 desktopName 属性。

除 file、 langaugeId、 rollback、 checkout、 checkin、 staycheckedout 和 offlineDirectory 之外的所有其他参数，也可以通过 Active Directory 组策略指定。有关此操作的详细信息，请参阅第 169 页上的第 8 章，“组件策略”。

注释 命令行属性将重写系统策略，而系统策略会重写用户策略。

View Client 配置文件

View Client 所需的连接选项可以在启动过程中从外部配置文件加载。文件必须为包含以下格式条目的 Unicode (UTF-16) 或 ASCII 文本文件：

```
-serverURL    <URL>
-userName     < 用户名 >
-domainName   < 域名 >
-password     < 密码 >
-desktopName  < 桌面名 >
```

要启动 View Client，以便其在启动时读取配置文件，请输入以下内容：

```
"C:\ProgramFiles\VMware\VMware View\Client\bin\wswc" -f < 文件名 >
```

虚拟打印

使用 View 的虚拟打印 (ThinPrint) 功能， View Client 和 View Client with Offline Desktop 用户可以从其远程系统内采用透明方式使用本地或网络的打印机，无需在每个 View 桌面中安装专用的打印机驱动程序。

注释 View Portal 不支持虚拟打印。

虚拟打印是一种即插即用的解决方案；打印机安装在本地系统之后，将自动添加到 View 桌面中的可用打印机列表中。无需进行进一步配置。

Virtual Printing 包含两大组件：驻留在 View Client 或 View Client with Offline Desktop 应用程序内的客户机组件 （.print Client）；属于 View 桌面的 View Agent 服务一部分的主机组件 （.print Engine）。打印作业由 .print Engine 通过 RDP 连接发送给 .print Client。

注释 在脱机桌面中， .print Engine 使用已命名的通道 （`Com1:`）将打印数据传输给 .print Client。

如果用户具有管理权限，也可以将打印机驱动程序安装在 View 桌面中；此操作不会影响 Virtual Printing 组件。

在 View 桌面中配置虚拟打印机实例

1 单击 **[Start （开始）]** > **[Settings （设置）]** > **[Printers and Faxes （打印机和传真）]**。随即显示 [Printers and Faxes （打印机和传真）] 窗口。

2 右键单击本地可用的任意打印机，并从上下文菜单中选择 **[Properties （属性）]**。随即显示与所选打印机相关的打印属性窗口。

3 选择 **[ThinPrint Device Setup （ThinPrint 设备设置）]** 选项卡。

4 使用滑块，选择压缩打印数据的选项：

- **[No images （无图像）]** － 仅打印文本。
- **[Extreme （极度）]** － 以可能的最大压缩率压缩图像，不考虑图像质量。
- **[Maximum （最大）]** － 在确保良好图像质量的前提下压缩图像。
- **[Optimal （最佳）]** － 在确保最佳图像质量的前提下压缩图像。
- **[Normal （正常）]** － 使用无失真图像压缩。

您可根据需要选择或取消选择 **[duplex （双面）]** 和 **[Show tray selection （显示送纸器选项）]** 复选框。

5 选择 **[General （常规）]** 选项卡，并单击 **[Printing Preferences （打印首选项）]**。

6 编辑页面和颜色设置；默认值来自主机打印机。

7 单击 **[Advanced （高级）]** 选项卡。如果主机中安装的打印机支持上述选项，请编辑以下设置以进行双面打印：[Long edge （长边）] 用于纵向打印， [Short edge （短边）] 用于横向打印。

要预览主机中的每一次打印输出，请启用 **[Preview on client before printing （打印前在客户端中预览）]**。从预览中，您可以使用任何打印机及其所有可用的属性。

8 单击 **[Adjustment （调整）]** 选项卡，查看自动打印调整选项。VMware 建议您保留默认设置。

9 单击 **[Apply （应用）]** 或 **[OK （确定）]**。单击 **[OK （确定）]** 以关闭打印属性窗口。

虚拟打印和 USB 打印

在 View 环境中，虚拟打印机和重定向 USB 打印机协同工作，不会出现冲突。

注释 重定向的 USB 打印机与本地 USB 端口相连接，并且从 View Client 内对其进行了手动重定向，从而可以与远程桌面进行通信。

如果用户将 USB 端口从本地系统重定向到远程桌面，那么在该远程系统 （假定安装了所需的驱动程序）上，可以使用与该端口相连接的所有 USB 打印机。

但是，由于重定向操作会有效地将 USB 打印机从本地环境中删除，其在远程系统上对应的虚拟部分也将被删除。

减少 Adobe Flash 带宽

您可以减少 Adobe Flash 内容在 View 桌面会话中运行时使用的带宽。减少带宽可以增强整体浏览体验，并且提高桌面上运行的其他应用程序的响应速度。

注释 只能在 Microsoft Windows 上的 Internet Explorer 会话中减少 Adobe Flash 带宽，而可减少带宽的版本也仅限于 Adobe Flash 版本 9 和 10。要利用减少 Adobe Flash 带宽的设置，不要在全屏幕模式下运行 Adobe Flash。

桌面用户可以重写桌面上的 Adobe Flash 设置。有关详细信息，请参阅第 115 页上的 "在桌面上重写带宽减少设置"。

设置 Adobe Flash 质量和调节

您可以为 Adobe Flash 内容指定可重写任意网页设置的允许的最高质量级别。如果给定网页的 Adobe Flash 质量高于允许的最高级别，则其质量将会减少到该指定的最高级别。较低的质量级别可以节省更多的带宽。可以使用以下 Adobe Flash 渲染质量模式：

- [Do not control （不进行控制）]：质量是由网页设置确定的。
- [Low （低）]
- [Medium （中）]
- [High （高）]

如果未指定最高质量级别，则系统默认值为 [Low （低）]。

Adobe Flash 使用计时器服务更新任意给定时间在屏幕上显示的内容。典型的 Adobe Flash 计时器间隔值为 4 到 50 毫秒之间。通过调节或延长此间隔，您可以减少帧速率，从而减少带宽。可以使用以下调节模式：

- [Disabled （禁用）]：不执行调节。不修改计时器间隔。
- [Conservative mode （保守模式）]：计时器间隔为 100 毫秒。此设置可以使丢帧数达到最小。
- [Moderate mode （中等模式）]：计时器间隔为 500 毫秒。
- [Aggressive mode （激进模式）]：计时器间隔为 2500 毫秒。此设置可使丢帧数达到最大。

无论选择哪种调节模式，音频速度都保持恒定不变。

配置 Adobe Flash 质量和调节

1. 在 View Administrator 中，单击 **[Edit （编辑）]**，然后选择 **[Desktop/Pool Settings （桌面 / 池设置）]**。
2. 从 **[Adobe Flash quality （Adobe Flash 质量）]** 下拉菜单中选择一个合适的质量模式。
3. 从 **[Adobe Flash throttling （Adobe Flash 调节）]** 下拉菜单中选择一个合适的调节模式。
4. 单击 **[Finish （完成）]**。

   所配置的设置将显示在 [Desktop/Pool Settings （桌面 / 池设置）] 窗格中。

注释 只有在 View Client 重新连接到桌面后，减少 Adobe Flash 带宽的设置才会生效。

在桌面上重写带宽减少设置

使用桌面上的光标，用户可以重写 Adobe Flash 内容显示设置。

在桌面上重写 Adobe Flash 设置

1. 在 Internet Explorer 中，浏览到相关的 Adobe Flash 内容，并在需要时启动该内容。

   根据 Adobe Flash 的设置配置，您会发现帧丢失或播放质量低。
2. 在播放 Adobe Flash 内容时，将光标移动至该内容中。

   只要光标停留在 Adobe Flash 内容中，其显示质量会不断提高。
3. 要保持提高的质量，请在 Adobe Flash 内容中双击。

客户端计算机信息

您可以配置 View Agent 的 `[CommandsToRunOnConnect]` 和 `[CommandsToRunOnReconnect]` 组策略设置，从而在用户连接和重新连接 View 桌面时将客户端计算机信息传送到 View Agent。View Agent 会将这些信息写入 View 桌面的注册表。利用第三方工具，您可以自定义的编写用这个信息去映射本地打印机到客户端计算机的脚本。

例如，如果要在用户连接 View 桌面时将客户端计算机的 IP 地址传送到 View Agent，可以启用 `[CommandsToRunOnConnect]` 组策略设置并将 `ViewClient_IP_Address` 命令添加到设置的命令列表中。有关更多信息，请参见第 176 页上的 “组策略对象”。

表 5-2 列出了发送到各种客户端类型的客户机代理的信息。第三方认证的客户端也可以提供客户端信息。

表 5-2. 桌面中提供的客户端信息

客户端信息	Windows	Wyse Thin OS	Linux	描述
ViewClient_IP_Address	X	X	X	客户端设备的 IP 地址。
ViewClient_MAC_Address	X	X	X	客户端设备的 MAC 地址。
ViewClient_Machine_Name	X	X	X	客户端设备的机器名称。
ViewClient_Machine_Domain	X		X	客户端设备的域。
ViewClient_LoggedOn_Username	X		X	在 View Client 中输入的用户名。
ViewClient_LoggedOn_Domainname	X			在 View Client 中输入的域。
ViewClient_Type	X	X	X	客户端设备的瘦客户端名或操作系统类型。
ViewClient_Broker_DNS_Name	X	X	X	View Connection Server 的 DNS 名称。
ViewClient_Broker_URL	X	X	X	View Connection Server 的 URL。
ViewClient_Broker_Tunneled	X	X	X	View Connection Server 的安全加密链路状态。此值为 [true] 或 [false]。
ViewClient_Broker_Tunnel_URL	X		X	如果 View Connection Server 的安全加密链路状态为 [true]，则指的是安全加密链路的 URL。
ViewClient_Broker_Remote_IP_Address	X	X	X	客户端的远程 IP 地址。

表 5-2. 桌面中提供的客户端信息 （续）

客户端信息	Windows	Wyse Thin OS	Linux	描述
ViewClient_TimeOffset_GMT	X	X	X	与 GMT 的时差，以 HH:MM 形式表达。 如果在 Windows 中使用 View Client，则无法从桌面注册表内的 Volatile Environment 或 View Agent 日志中获得此信息。此信息由专用通道发送。 **注释**：要禁用此项，请将 [Disable Time Zone Synchronization （禁用时区同步）] GPO 设置为 true。
ViewClient_TZID	X	X	X	Olson 时区 ID。 如果在 Windows 中使用 View Client，则无法从桌面注册表内的 Volatile Environment 或 View Agent 日志中获得此信息。此信息由专用通道发送。 **注释**：要禁用此项，请将 [Disable Time Zone Synchronization （禁用时区同步）] GPO 设置为 true。
ViewClient_Windows_Timezone	X	X	X	GMT 标准时间。 如果在 Windows 中使用 View Client，则无法从桌面注册表内的 Volatile Environment 或 View Agent 日志中获得此信息。此信息由专用通道发送。 **注释**：要禁用此项，请将 [Disable Time Zone Synchronization （禁用时区同步）] GPO 设置为 true。

注释 仅当使用 View Client 启动桌面时，才发送客户端的完整信息。当使用 View Portal 启动桌面时，不会显示以下注册表条目。

- `ViewClient_Machine_Name`
- `ViewClient_Machine_Domain`
- `ViewClient_IP_Address`
- `ViewClient_LoggedOn_Domainname`
- `ViewClient_LoggedOn_Username`
- `ViewClient_MAC_Address`
- `ViewClient_Type`

使用 PCoIP 显示协议

PCoIP 为 LAN 或 WAN 中的广大用户提供图像、音频和视频内容传送方面的最佳 PC 体验。PCoIP 可弥补因延迟增加或带宽减少导致的不便，确保最终用户在任何网络条件下均可保持高效。PCoIP 可以作为虚拟机和使用 Teradici 主机卡的物理机的 View 桌面的显示协议。

有关 PCoIP 系统要求的更多信息，请参见第 20 页上的 "PCoIP"。

如果要将虚拟桌面配置为采用 PCoIP 与 View Client 进行通信，请参见第 63 页上的第 4 章，"虚拟桌面部署"。

使用 HP RGS 显示协议

RGS 是一种来自 HP 的显示协议，允许用户通过标准网络访问远程计算机的桌面。您可以将桌面配置为使用 HP RGS 作为显示协议来运行，而不使用 RDP 或 PCoIP 协议。

注释 View Client 支持在连接 HP Blade PC、HP Workstation 和 HP Blade Workstation 时将 HP RGS 作为显示协议使用。目前尚不支持与运行于 ESX 上的虚拟机进行连接。

安装 HP RGS 组件

VMware View 未捆绑或许可 HP RGS。请与 HP 联系，获得 HP RGS 软件版本 5.2.5 的许可，以与 View 结合使用。

HP RGS 包含服务器端组件 （称为 RGS Sender）和客户端组件 （称为 RGS Receiver）。在配置 View 使用 HP RGS 之前，必须在远程桌面操作系统上安装 HP RGS Sender，在本地桌面上安装 HP RGS Receiver。请确保将 RGS Sender 应用程序或端口作为例外情况，添加到使用的任何防火墙软件中。默认的 RGS 端口是 42966。

有关如何安装并配置这些 HP RGS 组件的信息，请参见 HP RGS 文档，文档位置：http://www.hp.com。

警告 不要在 RGS Sender 或 RGS Receiver 上安装 RGS USB。

在 View Administrator 中配置 HP RGS

请确保您采用直接连接方式连接到 View Connection Server （关闭安全加密链路）。

验证是否采用了直接连接

1 在 View Administrator 中，单击 **[Configuration （配置）]**。
2 选择 **[Servers （服务器）]**，然后选择要配置的服务器。
3 单击 **[Edit （编辑）]**。
4 在 [Edit Server Settings （编辑服务器设置）] 对话框中，验证是否选中了 **[Direct connection to desktop （直接连接到桌面）]** 复选框。

如果要将虚拟桌面配置为采用 HP RGS 与 View Client 进行通信，请参见第 63 页上的第 4 章，“虚拟桌面部署”。

View Composer 6

View Composer 是一种功能丰富、具有高效存储能力的备选组件，用于创建和管理许多独立的虚拟机。本章对 View Composer 进行了概述。

以下内容将概述如何在 vCenter Server 中使用 View Composer 创建及使用 View Manager 管理链接克隆桌面，并介绍如何准备 vCenter Server 和用于 View Composer 部署的基础虚拟机映像。

本章讲述以下主题：

View Composer 概述

使用 View Composer 功能， View Manager 管理员可通过一个被称为 “父虚拟机” 的集中化基础映像快速地克隆和部署多个桌面。创建桌面后，桌面将间接地链接到父虚拟机中的快照。

这种链接之所以是间接链接，是因为首次创建一个或多个链接克隆时，系统还会创建父虚拟机的具有唯一标识的副本 （称为 “副本” ）。所有桌面克隆都直接绑定到该副本，而不是父虚拟机。此类桌面称为链接克隆桌面。

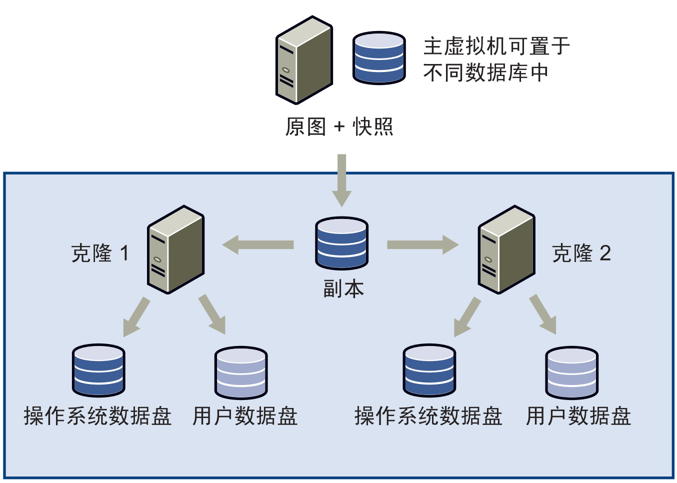
注释 在 vCenter Server 中，可通过副本虚拟机的 `replica-` 前缀及其后面的唯一 ID 识别副本虚拟机。

在 vSphere Client 4 中，副本虚拟机只会显示在 [Hosts and Clusters Inventory （主机和群集清单）] 视图中。在 VMware Infrastructure Client 3.5 中，副本虚拟机还会显示在 [Virtual Machines and Templates Inventory （虚拟机和模板清单）] 视图中。

更新或替换父虚拟机时，不会对链接克隆桌面产生直接影响，因此可将其视为独立虚拟机。图 6-1 中显示了这种关系。

注释 如果删除了副本，则绑定到该副本的桌面将停止工作；因此，副本成为 vCenter Server 中受保护的实体。

图 6-1. 父虚拟机、链接的副本和桌面克隆



由于此环境中所有链接克隆桌面均连接到公共源，因此， View Composer 可在维护用户无缝体验的同时，允许集中管理这些桌面。通过这种部署，可显著加快任务的执行，例如：将每个系统重置为默认配置、平衡存储、安装软件以及应用服务包。

通过在父虚拟机中执行上述活动，然后将链接克隆绑定到此配置的新快照， View Manager 管理员就可以同时更新 （或更改）所有链接克隆桌面的操作系统，安装或更新客户端应用程序，或修改桌面硬件设置。上述操作称为桌面重构。

注释 此外，所链接的克隆还可以绑定到完全不同的其他父虚拟机的新快照。

通过执行桌面刷新，管理员还可以将每个链接克隆桌面的操作系统数据 （可能在使用中被更改）返回至原始状态 （父虚拟机中的数据状态）。

在图 6-1 中，桌面用户数据已配置为驻留在单独的磁盘上，因此，不会受到桌面重构或桌面刷新操作的影响。这样，对系统的修改便可与用户数据存储设备相分离。

View Administrator 可提供高级概览视图，允许您查看正在执行的操作。策略可以控制执行哪些操作以及何时执行，从而最大程度地减少用户库的中断次数。如果某种更新会影响已连接的用户的会话，系统会在更新前使用自定义的消息通知这些用户。

链接克隆桌面的磁盘使用情况

由于操作系统和客户端应用程序都是从父虚拟机派生的，因此，链接克隆虚拟机最初占用的磁盘空间远低于完整克隆占用的磁盘空间。通过增量磁盘和精简部署，可显著降低操作系统和用户数据的存储开销。

在标准 （非链接克隆）自动化池中创建的每个新桌面都是基础模板的副本。结果，池中创建的每个克隆都复制基础模板的操作系统数据和用户数据，每个标准克隆所用的磁盘空间都与基础模板相同。

通过使用增量磁盘， View Composer 就可显著降低链接克隆桌面池的物理存储开销。增量磁盘是一种抽象存储机制，其逻辑大小可大于物理大小。精简型磁盘的增长取决于工作负载、关机策略、池类型等因素。

在部署链接克隆时，桌面使用增量磁盘来存储自身操作系统与父 虚拟机操作系统 （该桌面操作系统的来源）之间的数据差异。部署刚完成时，父虚拟机与链接克隆之间的差异极小；因此，增量磁盘也就极小。

由于每个桌面的增量磁盘不可避免地随着时间而增长，因此，在部署链接克隆时，您可以定义每个虚拟机允许的最大大小，将其限定到父虚拟机的原始大小。通常，存储链接克隆操作系统数据与父虚拟机操作系统数据之间差异所需的磁盘空间容量将远小于存储标准克隆所需的磁盘空间容量。如果增量磁盘的大小变得过大，则您可执行桌面刷新，将其返回到基准状态。

精简部署

为了将存储成本降至最低，操作系统数据磁盘和用户数据磁盘均使用一个称为 “Thin Provisioning （精简部署）” 的进程。使用此进程的磁盘所占据的空间不超过其所含数据需要的空间，从而减少了创建桌面后最初需要的物理磁盘容量。

注释 如果删除了数据，精简部署的磁盘的大小也不会减小。

存储过载

为新的链接克隆桌面池分配数据存储时，管理员可通过修改存储过载属性，来控制系统向数据存储中的可用空间分配新虚拟机的程度。

存储过载级别较低时，大部分可用空间将用作缓冲区，每个克隆的增量磁盘可在其中扩展。随着过载级别的增加，为单个增量磁盘增长预留的空间将随之减少，但数据存储中将容纳更多的虚拟机。

如果每个克隆都是一个完整的桌面，则存储过载级别用于计算超出克隆要使用的数据存储物理容量的那部分存储量。表 6-1 中显示了您可以设置的存储过载级别。

表 6-1. 存储过载级别

选项	存储过载级别
None （无）	存储尚未过载。
Conservative （保守）	数据存储大小的 4 倍。这是默认级别。
Moderate （中等）	数据存储大小的 7 倍。
Aggressive （激进）	数据存储大小的 15 倍。

如果存储过载级别过高，结果将导致为增量磁盘扩展预留的空间容量相对较少。但是，如果管理员预测到每个虚拟机的增量磁盘永远不会接近最大的可能大小，则可向数据存储中额外添加大量虚拟机。

虽然高过载级别可能是创建多个虚拟机的最佳选项，但管理员仍须密切关注此类桌面池，确保虚拟机的扩展并未完全消耗剩余的磁盘空间。通过定期刷新或重新平衡桌面池，并将操作系统数据大小降至基准水平，可以防止出现上述情况。

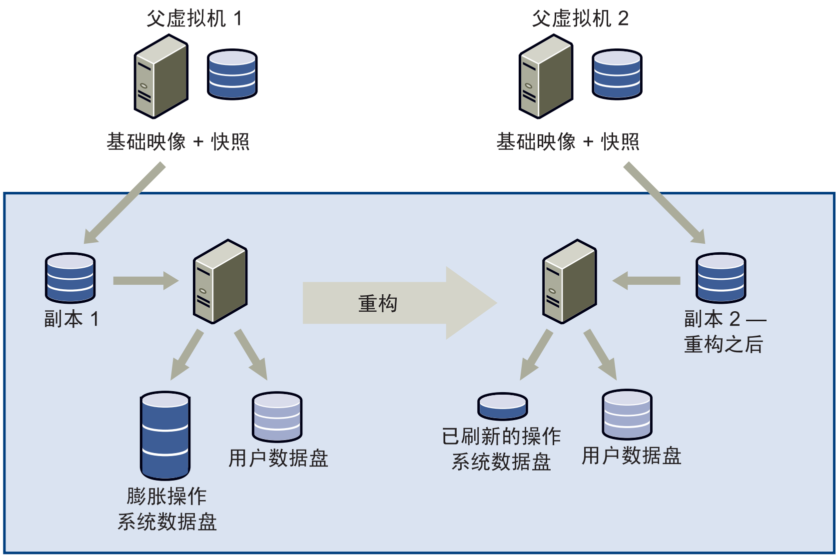
为处理每个数据存储的不同吞吐量级别，您可以为不同类型的数据存储 （如 NAS 和 SAN）分别指定不同的存储过载级别。

存储过载仅适用于增量磁盘。它不适用于用户磁盘或标准 （非链接）克隆。

桌面重构

在图 6-2 中，桌面克隆已链接到副本 1，副本 1 本身是父虚拟机 1 的副本。如果管理员在同一个或不同的父虚拟机中选择一个不同的快照 （如该示例所示），则系统将启动重构操作。无论何种情况，系统都会部署新的副本。

图 6-2. 桌面重构



副本 2 是父虚拟机 2 的完整副本。完成重构操作之后，桌面将绑定到副本 2，并会相应修改操作系统数据。完成重构之后，将减少桌面的操作系统数据量，但用户数据不受此事件的影响。

源虚拟机

在 VMware Infrastructure 3.5 中，通过使用 VirtualCenter Server 中另一个受保护的链接克隆桌面 （称为源虚拟机）可以加快重构过程。当您首次部署链接克隆桌面池时，源虚拟机会和副本一起创建。在 VMware Infrastructure 3.5 中，源虚拟机和副本均位于 VirtualCenter Server 中名为 `VMwareViewComposerReplicaFolder` 的文件夹内。

注释 VMware vSphere 4 对克隆过程进行了优化，因此不需要创建源虚拟机。

发生重构事件时，源虚拟机是根据新快照进行重构的第一个桌面。 View Composer 从 VirtualCenter Server 中删除现有的链接克隆桌面池，然后根据需要多次复制源虚拟机，以便将其替换。

这种生成池的方法可优化重构过程，与分别重构池中每个链接克隆桌面相比，这种方法更快捷。

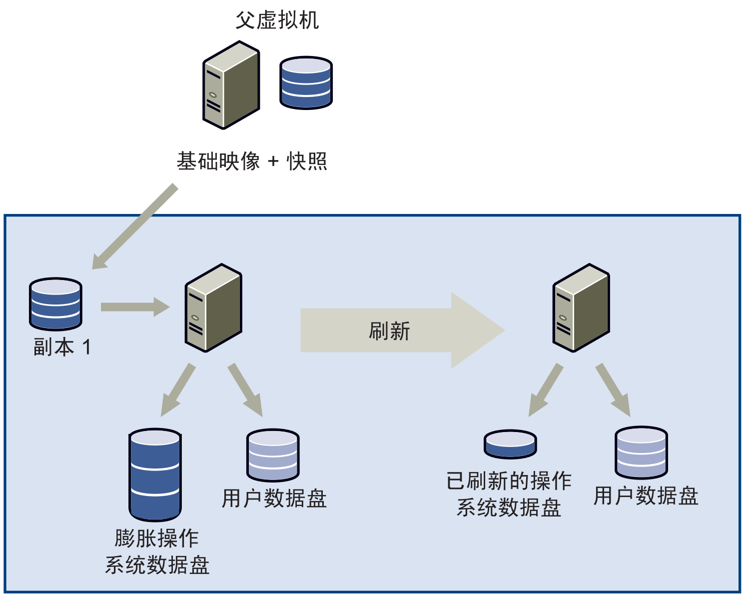
桌面刷新

桌面刷新与桌面重构类似，但它不会对基础映像进行任何更改。执行此操作旨在将桌面池的系统数据恢复到基准状态，从而减少所链接的每个克隆的操作系统数据量。

注释 桌面刷新不适用于包含用户数据的精简部署的磁盘。

桌面刷新既可根据需要定时执行，也可以在操作系统数据达到指定量时执行。图 6-3 显示了此操作的影响。请注意，用户数据磁盘不受此事件的影响。

图 6-3. 桌面刷新



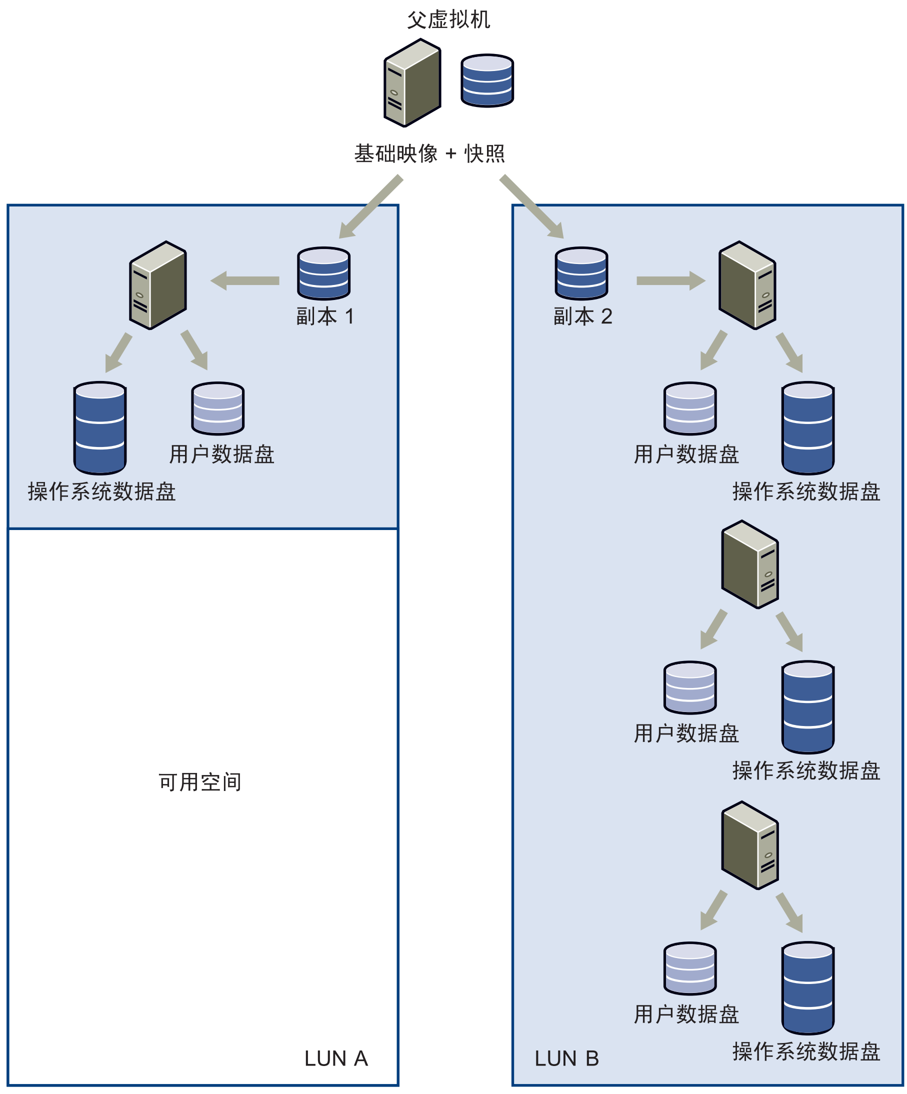
您应偶尔刷新连接的系统，以防止桌面克隆增加到完整虚拟机大小，这至关重要。如果不检查所有绑定的虚拟机，任其自行增长，则它们将迅速占用数据存储中剩余的所有可用空间，当存储过载级别较高时尤其如此。

桌面重新平衡

逻辑驱动器是指在阵列 （在一组驱动器上定义的数据存储子系统）上创建的一种结构。逻辑驱动器是阵列的逻辑分段，它们通常称作 LUN 即逻辑单元号 （Logical Unit Number）， LUN 提供了主机用来访问逻辑驱动器的标识符。

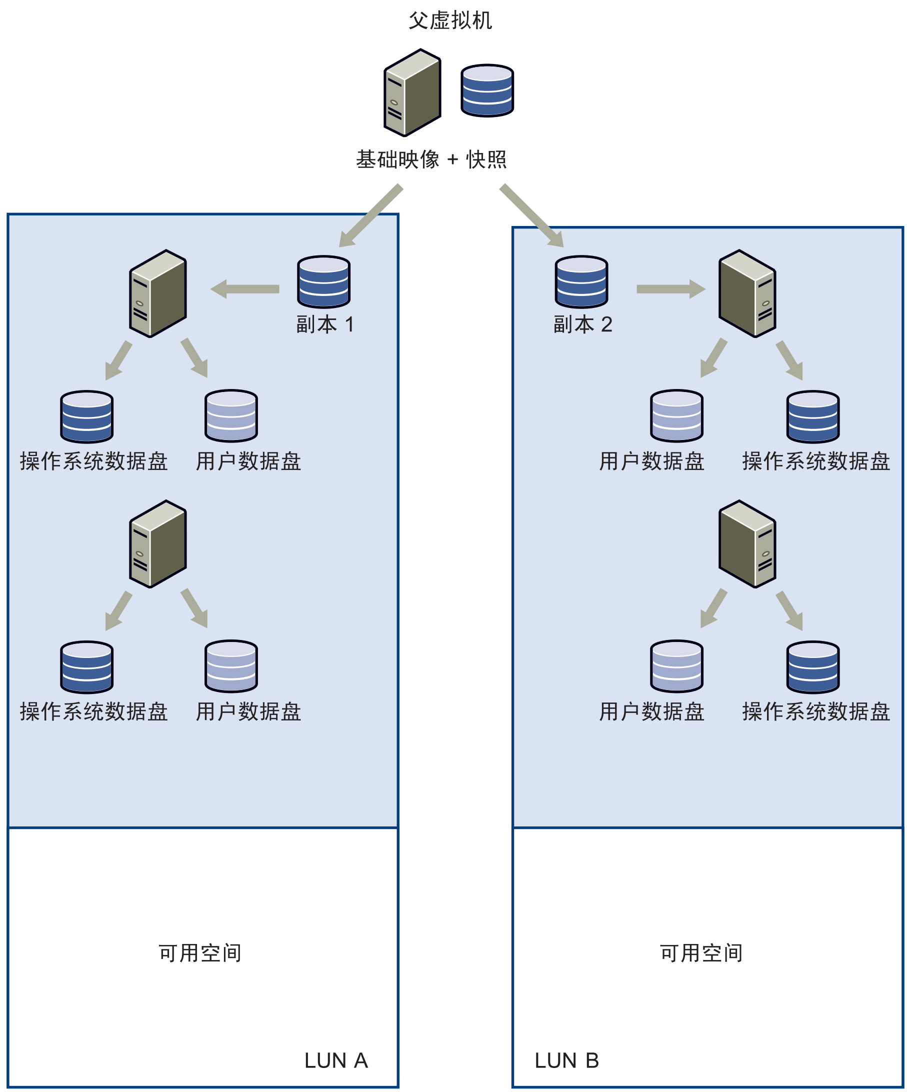
管理员创建大型桌面池并使用多个 LUN 时，如果初始大小不准确，则可能会导致无法有效利用空间。图 6-4 显示了许多在两个 LUN 之间未均匀分布的虚拟桌面。

图 6-4. 重新平衡桌面之前的状况



重新平衡 LUN 后，任何选定的（或所有）虚拟机将在可用逻辑驱动器之间均匀分布。图 6-5 中显示了重新平衡后的效果。

图 6-5. 重新平衡桌面之后的状况



如果存储过载级别过高，可能会导致虚拟机进一步增加，直至占用数据存储内的所有可用空间。虚拟机在数据存储中占用不同的空间数量时，系统的响应也有所不同：

- 95%：系统将生成日志条目，指出数据存储可用空间不足。
- 99%：数据存储内的每个虚拟机都将挂起。

重新平衡功能为管理员提供了一种理想机制，允许管理员向数据存储引入其他存储，防止出现第二种结果。此外，在执行重新平衡操作之前，您还可以撤销原有的存储设备并更改资源池和主机。

只能重新平衡处于 [Ready （就绪）]、 [Error （错误）] 或 [Customizing （自定义）] 状态且未计划取消或等待取消的桌面。此外，您无法在多台独立 ESX 主机中的本地存储系统之间重新平衡负载。

建议您在数据存储中保留链接克隆桌面虚拟机、而不保留其他类型的虚拟机，这样，您可对所有虚拟机应用重新平衡操作。

注释 为了重新平衡桌面，View Manager 必须根据当前的基础映像自动刷新操作系统，并将系统数据返回到基准状态。但如果用户数据位于单独的用户数据磁盘中，则不会受到影响。

永久桌面池和非永久桌面池

永久桌面池和非永久桌面池配置均受 View Composer 支持。在永久配置中，专用磁盘（指用来存储操作系统数据的系统磁盘以及用来存储用户数据的用户磁盘）可将操作系统数据和用户数据分开。这样，可确保即使在重构或刷新操作系统时，用户数据也不会受到影响。

在非永久配置中，用户数据是临时数据，因此，操作系统数据和用户数据均存储在系统磁盘中。在这种配置中，如果重构或刷新系统，用户数据不会受到保护。

注释 您可将永久桌面设置为在用户注销时自动刷新。这有助于最大程度地减少池的空间要求。同样，也可将非永久池设置为首次使用之后删除，从而整体上减少池中非活动桌面的数目。

使用 QuickPrep 进行链接克隆桌面部署

QuickPrep 是 View Composer 在部署链接克隆桌面时使用的系统工具。 QuickPrep 可对通过父虚拟机创建的每个桌面进行个性化设置。

在初次启动每个新桌面的过程中， QuickPrep 会确保为系统指定一个新名称 （在部署过程中指定）并确保其加入到适当的域。QuickPrep 还用于装载要包含用户配置文件信息的新卷。在这些步骤中，需要重新启动两次链接克隆。此外， QuickPrep 还将在 Active Directory 域控制器中创建与每个桌面对应的新计算机帐户。在桌面刷新之后，上述事件也会发生。

您必须在 Active Directory 中创建一个域用户帐户，以供 View Composer 服务使用。View Composer 需要使用该帐户将链接克隆桌面加入到域中。当您为 vCenter Server 配置 View Composer 以及配置和部署链接克隆桌面池时，要指定域用户帐户。您需要在 Active Directory 中为域用户帐户添加 "创建计算机对象" 和 "删除计算机对象" 的权限。这些权限允许用户在指定的 Active Directory 容器中添加和删除计算机对象。您应当为 View Composer 专门创建域用户帐户。您可以使用现有的域用户帐户，但这个帐户最好是唯一的。

创建、刷新或重构桌面之后，可在每个重新同步的桌面上运行用户定义的自定义脚本，以便执行其他操作。在关闭桌面之前，也可以立即在其中运行脚本。在初次部署链接克隆桌面的最后阶段，您可以提供每种脚本 （必须是父虚拟机中的脚本）的路径。QuickPrep 负责确保在上述任何一种情况下均执行这些脚本。

针对 View Composer 准备 vCenter Server

在部署链接克隆桌面之前，您必须先配置 VMware vCenter Server，以便做好充分准备，顺利使用 View Composer 服务从父虚拟机中创建副本和链接克隆桌面。

- View Composer 服务必须本地安装在 vCenter Server 中。
- 您可以在混合包含了 ESX/ESXi 4 主机和 ESX/ESXi 3.5 主机的群集上部署一个链接克隆桌面池，直到您设置了 **[vSphere]** 模式。
- Active Directory 管理员必须创建一个具有必要权限级别的用户，以便 View Composer 服务软件使用该用户身份创建链接克隆桌面并将其添加到域中。请参阅 第 130 页上的 "使用 QuickPrep 进行链接克隆桌面部署"。
- 如果 View Manager 使用的 vCenter Server 用户不是管理员，则您必须扩展他的角色，使其拥有 View Composer 服务软件所需的 vCenter Server 权限。
- 如果 vCenter Server 内没有可用的资源池，您必须在要存储链接克隆桌面的 ESX 主机或群集中创建一个资源池。有关详细信息，请参见 vCenter Server 文档。

- 如果您的网络环境内没有 View Composer 数据库，则必须创建一个数据库和数据源名称（Data Source Name，DSN）来存储 View Composer 数据。如果您的环境中已存在 View Composer 数据库，请参见第 152 页上的 “使用现有 View Composer 数据库”，以获取有关如何使用该数据源的补充信息。

注释 如果数据库实例不在 vCenter Server 中，也不在网络环境中的其他位置，您必须安装一个数据库实例。 View Composer 服务的安装程序不提供数据库。

请参见第 25 页上的表 1-3，“View Composer 的数据库支持和要求”，以获取受支持的数据库的相关信息。根据所使用的数据库类型，请按照以下某一部分中的说明进行操作：

- 要配置 SQL Server 数据库，请按照第 131 页上的 “为 View Composer 创建 SQL Server 数据库和数据源” 中的说明进行操作。
- 要配置 Oracle 9i 数据库，请按照第 133 页上的 “为 View Composer 创建 Oracle 9i 数据库和数据源” 中的说明进行操作。
- 要配置 Oracle 10g 数据库，请按照第 135 页上的 “为 View Composer 创建 Oracle 10g 数据库和数据源” 中的说明进行操作。

为 View Composer 创建 SQL Server 数据库和数据源

本部分介绍如何在现有 SQL Server 实例中添加新的 View Composer 数据库，以及如何使这个数据源对该主机系统上运行的所有其他组件都可见。

所有说明均假定 vCenter Server 主机或您的网络环境中已经安装了 Microsoft SQL Server 2005，且您使用 SQL Server Management Studio Express 创建和管理数据源。如果该数据库与 vCenter Server 位于同一系统中，则您可以使用集成 Windows 身份验证 （Integrated Windows Authentication）安全模式。如果数据库位于远程系统中，则无法使用这种身份验证模式。

以下说明还假定您要在 Windows Server 2003 SP2 或更高版本上配置该数据库。如果您要在 Windows XP Professional SP2 主机上配置 ODBC 数据源，则某些步骤会有所不同。

可从以下网站获取 SQL Server Management Studio Express：

http://www.microsoft.com/downloadS/details.aspx?familyid=C243A5AE-4BD1-4E3D-94B8-5A0F62BF7796

将 View Composer 数据库添加到 SQL Server 2005 中

1 在 vCenter Server 主机系统中，选择 **[Start （开始）]** > **[All Programs （所有程序）]** > **[Microsoft SQL Server 2005]** > **[SQL Server Management Studio Express]**，然后连接到 Virtual Infrastructure Management 的现有 SQL Server 实例。

2 在 [Object Explorer （对象浏览器）] 窗格中，右键单击 **[Databases （数据库）]** 条目并选择 **[New Database （新建数据库）]**。随即将显示 **[New Database （新建数据库）]** 对话框。

3 在 **[Database name （数据库名称）]** 字段中输入一个名称 （例如 `ViewComposer`），然后单击 **[OK （确定）]**。数据库将添加到 [Object Explorer （对象浏览器）] 中的 **[Databases （数据库）]** 条目下。

4 退出 Microsoft SQL Server Management Studio Express。

添加 ODBC 数据源

1 在 vCenter Server 主机系统中，选择 **[Start （开始）]** > **[Administrative Tools （管理工具）]** > **[Data Source (ODBC) （数据源 （ODBC））]**。随即显示 [Microsoft ODBC Data Source Administrator（Microsoft ODBC 数据源管理器）] 向导。

2 选择 **[System DSN （系统 DSN）]** 选项卡。

3 单击 **[Add （添加）]**，然后从列表中选择 **[SQL Native Client （SQL 本地客户端）]**。

4 单击 **[Finish （完成）]**。随即显示 [Create a New Data Source to SQL Server （创建 SQL Server 的新数据源）] 设置向导。

5 在相应字段中，输入 View Composer 数据库的名称 （例如 `VMware View Composer`）和简要描述。

6 在 **[Server （服务器）]** 字段中，以 **< 主机名称 >\< 服务器名称 >** 格式输入 SQL Server 数据库的信息，其中 **< 主机名称 >** 是指主机系统的名称，**< 服务器名称 >** 是指 SQL Server 实例。例如：

```
VCHOST1\SQLEXP_VIM
```

单击 **[Next （下一步）]**。

7 请确保已选中 **[Connect to SQL Server to obtain default settings for the additional configuration options （连接到 SQL Server 以获得其他配置选项的默认设置）]** 复选框，并选择下列选项之一：

- 如果使用本地 SQL Server，请选择 **[Windows NT authentication （Windows NT 身份验证）]**。它也称为 "受信任的身份验证"，仅当 SQL Server 在 vCenter Server 主机上运行时，才支持这种验证。
- 如果您使用远程 SQL Server，请选择 **[SQL Server authentication （SQL Server 身份验证）]**。Windows NT 身份验证在远程 SQL Server 中不受支持。

单击 **[Next （下一步）]**。

8 选中 **[Change the default database to （将默认数据库更改为）]** 复选框，并从相关列表中选择您已为 View Composer 创建的数据库的名称 （在此示例中，名称是 `ViewComposer`）。单击 **[Next （下一步）]**。

9 单击 **[Finish （完成）]** > **[OK （确定）]**。

10 单击 **[OK （确定）]** 以关闭 [Microsoft ODBC Data Source Administrator （Microsoft ODBC 数据源管理器）] 向导。

为 View Composer 创建 Oracle 9i 数据库和数据源

以下内容介绍如何在现有 Oracle 9i 实例中添加新的 View Composer 数据库，以及如何使这个数据源对该主机系统上运行的所有其他组件都可见。

所有说明均假定 vCenter Server 主机上已安装了 Oracle 9i。以下说明还假定您要在 Windows Server 2003 SP2 或更高版本上配置该数据库。如果您要在 Windows XP Professional SP2 主机上配置 ODBC 数据源，则某些步骤会有所不同。

将 View Composer 数据库添加到 Oracle 9i 中

1 在 vCenter Server 主机中，选择 **[Start （开始）]** > **[All Programs （所有程序）]** > **[Oracle-OraHome92]** > **[Configuration and Migration Tools （配置和迁移工具）]** > **[Database Configuration Assistant （数据库配置助理）]** 启动 Oracle Database Configuration Assistant。

2 显示 [Welcome （欢迎）] 页面时，请单击 **[Next （下一步）]**。

3 在 [Operations （操作）] 页面上，选择 **[Create a database （创建数据库）]**，然后单击 **[Next （下一步）]**。

4 在 [Database Templates （数据库模板）] 页面上，选择 **[Data Warehouse （数据仓库）]** 模板，然后单击 **[Next （下一步）]**。

5 在 [Database Identification （数据库标识）] 页面上，输入全局数据库名称和 Oracle 系统标识符 （System Identifier， SID）前缀。

为简化这一过程，您可以为这两项输入相同的值。

6 在 [Database Connection Options （数据库连接选项）] 页面上，选择 **[Dedicated Server Mode （专用服务器模式）]**。

7 在其余的配置页面上，均单击 **[Next （下一步）]** 接受默认设置。

8 在 [Creation Options （创建选项）] 页面上，请验证是否已选中 **[Create Database （创建数据库）]** 选项并单击 **[Finish （完成）]**。

9 复查 [Summary （摘要）] 页面上的选项，然后单击 **[OK （确定）]** 以创建数据库。

数据库即可被创建。

10 为 SYS 和 SYSTEM 系统管理员帐户设置密码。

使用 SYSTEM 帐户设置数据源连接。

添加 ODBC 数据源

1 在 vCenter Server 主机中，选择 **[Start （开始）]** > **[Administrative Tools （管理工具）]** > **[Data Source (ODBC) （数据源 （ODBC））]**。随即显示 [Microsoft ODBC Data Source Administrator （Microsoft ODBC 数据源管理器）] 向导。

2 选择 **[System DSN （系统 DSN）]** 选项卡。

3 单击 **[Add （添加）]**，然后从列表中选择适当的 Oracle 驱动程序 （例如 `Oracle in OraHome92`）。

4 单击 **[Finish （完成）]**。随即显示 [Oracle ODBC Driver Configuration （Oracle ODBC 驱动程序配置）] 对话框。

5 输入要用于 View Compose 的 DSN、对该数据源的描述以及用户 ID 以连接到数据库。

注释 安装 View Composer 的过程中，您会使用该 DSN。

对于 **[TNS Service Name （TNS 服务名）]** 来说，请从下拉菜单中选择 [Global Database Name （全局数据库名称）] （在 Oracle Database Configuration Assistant 中指定）。

6 单击 **[Test Connection （测试连接）]** 以验证此数据源，然后单击 **[OK （确定）]**。

为 View Composer 创建 Oracle 10g 数据库和数据源

以下内容介绍如何在现有 Oracle 10g 实例中添加新的 View Composer 数据库，以及如何使这个数据源对该主机系统上运行的所有其他组件都可见。

所有说明均假定 vCenter Server 主机上已安装了 Oracle 10g。以下说明还假定您要在 Windows Server 2003 SP2 或更高版本上配置该数据库。如果您要在 Windows XP Professional SP2 主机上配置 ODBC 数据源，则某些步骤会有所不同。

将 View Composer 数据库添加到 Oracle 10g 中

1 在 vCenter Server 主机中，选择 **[Start（开始）]** > **[All Programs（所有程序）]** > **[Oracle-OraDb10g_home]** > **[Configuration and Migration Tools （配置和迁移工具）]** > **[Database Configuration Assistant （数据库配置助理）]** 启动 Oracle Database Configuration Assistant。

2 显示 [Welcome （欢迎）] 页面时，请单击 **[Next （下一步）]**。

3 在 [Operations （操作）] 页面上，选择 **[Create a database （创建数据库）]**，然后单击 **[Next （下一步）]**。

4 在 [Database Templates （数据库模板）] 页面上，选择 **[Data Warehouse （数据仓库）]** 模板，然后单击 **[Next （下一步）]**。

5 在 [Database Identification （数据库标识）] 页面上，输入全局数据库名称和 Oracle 系统标识符 （System Identifier， SID）前缀。

   为简化这一过程，您可以为这两项输入相同的值。

6 在 [Management Options （管理选项）] 页面上，单击 **[Next （下一步）]** 接受默认设置。

7 在 [Database Credentials （数据库凭据）] 页面上，输入系统帐户的密码，然后单击 **[Next （下一步）]**。

8 在其余的配置页面上，均单击 **[Next （下一步）]** 接受默认设置。

9 在 [Creation Options （创建选项）] 页面上，请验证是否已选中 **[Create Database （创建数据库）]** 选项并单击 **[Finish （完成）]**。

10 复查 [Confirmation （确认）] 页面上的选项，然后单击 **[OK （确定）]** 以创建数据库。

   数据库即可被创建。

11 单击 **[Finish （完成）]**。

添加 ODBC 数据源

1 在 vCenter Server 主机中，选择 **[Start （开始）]** > **[Administrative Tools （管理工具）]** > **[Data Source (ODBC) （数据源 （ODBC））]**。随即显示 [Microsoft ODBC Data Source Administrator （Microsoft ODBC 数据源管理器）] 向导。

2 选择 **[System DSN （系统 DSN）]** 选项卡。

3 单击 **[Add （添加）]**，然后从列表中选择适当的 Oracle 驱动程序 （例如 `Oracle in OraDb10g_home`）。

4 单击 **[Finish （完成）]**。随即显示 [Oracle ODBC Driver Configuration （Oracle ODBC 驱动程序配置）] 对话框。

5 输入要用于 View Compose 的 DSN、对该数据源的描述以及用户 ID 以连接到数据库。

注释 安装 View Composer 的过程中，您会使用该 DSN。

对于 **[TNS Service Name （TNS 服务名）]** 来说，请从下拉菜单中选择 [Global Database Name （全局数据库名称）] （在 Oracle Database Configuration Assistant 中指定）。

6 单击 **[Test Connection （测试连接）]** 以验证此数据源，然后单击 **[OK （确定）]**。

向 vCenter Server 添加 View Composer 服务

View Manager 使用 View Composer 从 vCenter Server 中创建和部署链接克隆桌面。在安装 View Composer 服务软件的过程中，您可以指定该服务软件用来与 View Connection Server 进行通信的端口。如果 vCenter Server 主机中运行了 Windows 防火墙，则您必须将此端口添加到例外列表中或停用本地防火墙服务。

以下步骤介绍如何在 vCenter Server 中安装 View Composer 服务，以及如何将其配置为使用专用于存储链接克隆的数据源。

安装 View Composer 服务

1 运行 View Composer 服务安装程序，其中 xxx 是指可执行文件的内部版本号：

```
VMware-viewcomposer-xxx.exe
```

2 接受 VMware 许可条款并单击 **[Next （下一步）]**。

3 接受或更改目标文件夹路径，并单击 **[Next （下一步）]**。

4 在 **[Datasource Name （数据源名称）]** 字段中，输入您在 [Microsoft ODBC Data Source Administrator （Microsoft ODBC 数据源管理器）] 向导中提供的数据库名称 （在上例中，名称为 `VMware View Composer`）。

5 请在显示的字段中输入域管理员的用户名和密码，并单击 **[Next （下一步）]**。

6 选中 **[Create a new RSA key container （创建新的 RSA 密钥容器）]** 单选按钮。创建 RSA 密钥对的目的是：对要存储在 View Composer 数据库中的 Active Directory 身份验证信息进行加密和解密。单击 **[Next （下一步）]**。

7 输入端口值或使用默认值，然后选中 **[Create default SSL certificate （创建默认 SSL 证书）]** 单选按钮。单击 **[Next （下一步）]**。

8 请单击 **[Install （安装）]** 开始安装。完成安装后，单击 **[Finish （完成）]**。

vCenter Server 用户权限

如果 View Manager 用户在 vCenter Server 中不是管理员，则您必须向 vCenter Server 用户条目分配角色，以便向其授予创建并管理对象所需的适当权限级别。

除了要启用第 36 页上的 "View Manager 用户的 vCenter Server 权限" 中所述的标准权限以外， View Composer 服务软件还要求您启用表 6-2 中列出的附加权限。

表 6-2. 创建 View Composer 角色：所需权限

权限组	要启用的权限
Folder （文件夹）	**Create Folder** （创建文件夹）
Datastore （数据存储）	**Browse Datastore** （浏览数据存储） **File Management** （文件管理）
Virtual Machine （虚拟机）	**Inventory** （清单） **Configuration** （配置） **State** （状态） **Provisioning** （部署） > **Clone** （克隆） **Provisioning** （部署） > **Allow Disk Access** （允许磁盘访问）
Resource （资源）	**Assign Virtual Machine To Resource Pool** （将虚拟机分配给资源池）
Global （全局）	**Enable Methods** （启用方法） **Disable Methods** （禁用方法）

注释 vCenter Server 中的管理用户默认具有所有这些必备权限。

本地系统管理员

View Composer 要求 vCenter Server 用户也是安装该服务的计算机（即 vCenter Server）的系统管理员。为了满足此要求， View Manager 用来部署链接克隆桌面的任何 vCenter Server 用户都必须是 vCenter Server 中本地系统 [Administrators （管理员）] 组的成员。

准备父虚拟机

链接克隆桌面将使用父虚拟机作为基础映像。要使 View Manager 在链接克隆桌面部署中使用父虚拟机，您必须先在父虚拟机的操作系统中安装 View Agent。

请确保您对父虚拟机具有管理权限，且已安装以下必备组件。请确保父虚拟机满足以下条件：

- 已加入要放置链接克隆桌面的 Active Directory 域中。
- 已正确配置网络设置 （代理等）。
- 使用 DHCP 以获得其 IP 地址。
- 系统磁盘将连接到 SCSI （0:0）虚拟设备节点。此属性可从 vCenter Server 内进行配置。
- 操作系统的电源设置始终设为 [On （打开）]。
- 系统磁盘包含单个卷 （支持多个虚拟磁盘）。

警告 请勿从因磁盘分区而产生多个卷的父虚拟机中部署克隆。 View Composer 服务不支持多个分区。

- View Agent 服务软件已安装且正在运行。

  注释 要在大型环境中自动更新 View Agent， VMware 建议使用标准的 Windows 更新机制，例如 Altiris、 SMS、 LanDesk、 BMC 或其他系统管理软件。

如果您尚未满足此条件，请在父虚拟机中安装最新的操作系统、应用程序服务包和修补程序。

删除 DHCP 租期

建议您释放父虚拟机中可能存在的任何 DHCP 信息，这样，就不会在池内链接克隆之间复制租赁的 IP 地址。通过在父虚拟机中打开命令提示符并输入以下内容，您可以释放 DHCP 租期：

```
ipconfig /release
```

在父虚拟机中安装 View Agent

如果没有安装 View Agent，则必须在父虚拟机中安装它，以便允许 View Connection Server 与使用基础映像创建的桌面克隆进行通信。

安装 View Agent

1 在客户系统上运行以下可执行文件，其中 xxxxxx 是指文件的内部版本号：

```
VMware-viewagent-xxxxxx.exe
```

2 显示 [VMware Installation （VMware 安装）] 向导时，请单击 **[Next （下一步）]**。

3 接受 VMware 许可条款并单击 **[Next （下一步）]**。

4 选择自定义的安装选项。您必须安装 **View Composer Agent**。

您还可以选择或取消选择以下功能：

- 如果您希望允许用户从 View Connection Server 下载其虚拟桌面的副本，并用于笔记本电脑等本地计算机设备，请安装 **Offline Desktop** 组件。

  vSphere 4 不支持 Offline Desktop。Offline Desktop 是一项试验性功能。有关试验性功能的详细信息，请参阅第 14 页上的 “系统要求”。

- 如果虚拟桌面用户需要使用虚拟桌面访问本地连接的 USB 设备，请安装 **USB Redirection** 组件。

  注释 Windows 2000 不支持 USB 重定向。

- 如果要启用单点登录 （Single Sign-on， SSO），请安装 **View Secure Authentication** 组件。

  如果启用了该功能，用户在登录 View Client 时不会收到重新输入身份验证信息的提示，即可登录到虚拟桌面。

- 如果在事先未安装其他驱动的情况下，让用户在虚拟桌面使用客户系统的打印机，请安装 **Virtual Printing** 组件。请参阅第 112 页上的 “虚拟打印”。

- 如果希望用户通过 PCoIP 显示协议进行连接，请安装 **PCoIP Server** 组件。PCoIP 为 LAN 或 WAN 中的广大用户提供图像、音频和视频内容传送方面的最佳 PC 体验。

  注释 在 Windows Vista 中，如果您安装了 **PCoIP Server** 组件，则 Windows 组策略 **[Disable or enable software Secure Attention Sequence （禁用或启用软件安全注意序列）]** 将被启用并设置为 [`Services and Ease of Access applications` （服务和轻松访问应用程序）]。如果更改此设置，单点登录功能将无法正常工作。

5 接受或更改目标文件夹，并单击 **[Next （下一步）]**。

6 请单击 **[Install （安装）]** 开始安装。

7 完成安装后，单击 **[Finish （完成）]**。

创建父虚拟机快照

在基础映像中安装 View Agent 之后，您必须使用 vCenter Server 拍摄处于关闭状态的系统快照。此快照将用作绑定到父虚拟机的第一组链接克隆桌面的基准配置。

注释 拍摄快照之前，必须完全关闭父虚拟机。

从 View Manager 中部署链接克隆桌面

仅当 View Manager 能够与运行 View Composer 服务、且已正确配置的 vCenter Server 主机进行通信时，才可部署链接克隆桌面。此外， Active Directory 林必须具有主机域名全称 （例如 `example.com`）。如果环境中的域控制器名称未限定，则无法使用 View Composer。

在尝试创建新的链接克隆桌面池之前，必须先确保 View Manager 可与 vCenter Server 通信，且已启动 View Composer 服务软件。建立连接之后，您将能够部署新的链接克隆桌面池。

警告 在部署之前或部署过程中，请勿从 vCenter Server 内修改父虚拟机 （例如，将其转换为模板）。 View Composer 服务软件要求父虚拟机在此操作过程中保持不变。

在 View Manager 中添加或编辑 vCenter Server 条目

1 从 View Administrator 内单击 **[Configuration （配置）]**，以显示 [Configuration （配置）] 视图。

2 在 [vCenter Server] 下，（如果您尚未执行此操作）请单击 **[Add （添加）]**，并填写要与 View Manager 结合使用的 vCenter Server 的详细信息：

   a 在 **[Server address （服务器地址）]** 文本框中，输入要与 View Manager 通信的 VMware vCenter Server 的 FQDN 或 IP 地址。

> **警告** 如果通过 DNS 名称或 URL 输入服务器，则系统将不执行任何 DNS 查找以验证先前是否曾使用 IP 地址输入该服务器。如果同时使用 DNS 名称和 IP 地址添加 vCenter Server，则会发生冲突。

   b 在 **[User name （用户名）]** 文本框中，输入 vCenter Server 用户的名称。

   c 在 **[Password （密码）]** 文本框中，输入与以上输入的用户对应的密码。

   d （可选）在 **[Description （说明）]** 文本框中，输入此 vCenter Server 的描述。

   e 如果要通过安全通道 （SSL）连接到 vCenter Server，确保已选中 **[Connect using SSL （使用 SSL 连接）]** 复选框。这是默认设置。

   f 在 [Port （端口）] 文本框中，输入 TCP 端口号。默认端口号为 443。

   如果已显示所需的 vCenter Server，请选中该条目并单击 **[Edit （编辑）]**。随即显示 vCenter Server 设置列表。

3 单击 **[Check for View Composer Compatibility （检查 View Composer 的兼容性）]** 按钮，以检查 vCenter Server 上是否正在运行 View Composer 服务。如果检查成功，则会显示 [View Composer Settings （View Composer 设置）] 属性组。

4 请确保已选中 **[Enable View Composer （启用 View Composer）]** 复选框，以及在 vCenter Server 主机中安装 View Composer 服务时所指定的端口与该端口号相符。

5 单击 **[Add（添加）]**，以在 **[Add QuickPrep Domain（添加 QuickPrep 域）]** 对话框中输入所需的详细信息：

   输入 Active Directory 域的主机域名全称 （例如 domain.com）；输入用户名，其中要包含此主机域名全称 （例如 domain.com\admin）；输入特定用户的密码。

   注释 所提供的凭据必须代表一个域帐户（由 Active Directory 管理员创建），该域帐户有权在指定的 Active Directory 容器中添加和删除计算机对象。请参阅第 130 页上的 "使用 QuickPrep 进行链接克隆桌面部署"。

   View Composer 不对您输入的设置进行验证。

   View Composer 会使用所添加的域和相关的用户凭据，将链接克隆加入到域中。

6 单击 **[Add （添加）]** > **[OK （确定）]**。

   View Composer 用户将添加到 **[QuickPrep domains （QuickPrep 域）]** 列表中。

7 单击 **[OK （确定）]** 以关闭 vCenter Server 设置窗口。

配置和部署新的链接克隆桌面池

1 从 View Administrator 内单击 **[Desktops （桌面）]** 按钮，然后单击 **[Inventory（清单）]** 选项卡。在 **[Desktops （桌面）]** 窗格中，请确保选中 **[Desktops （桌面）]** 选项卡，并单击 **[Add （添加）]**。

2 随即显示 [Add Desktop （添加桌面）] 向导。在此向导中，您可以配置和部署新的链接克隆桌面池。选择 **[Automated Desktop Pool （自动桌面池）]**，并单击 **[Next （下一步）]**。

3 选择要创建的桌面池类型，并单击 **[Next （下一步）]**。

池类型	描述
Persistent（永久）	这种类型的桌面池中的桌面是静态分配的，以确保用户每次登录时都能连接到同一系统。在用户首次连接时，就会进行桌面分配。
Non-persistent（非永久）	此类池中的桌面是在用户登录时以动态方式分配的，并在用户断开连接时返回到池中。

4 选择此桌面要使用的 vCenter Server，并确保已选中 **[Use linked clone technology to create desktops in this pool （使用链接克隆技术在此池中创建桌面）]** 选项。单击 **[Next （下一步）]**。

5 请输入 **[Desktop ID （桌面 ID）]**，并可选择输入 **[Desktop Display Name （桌面显示名称）]** 和 **[Description （描述）]**。

桌面 ID 是 View Manager 用来识别桌面池的标识，也是用户在登录时看到的名称。您可随意指定桌面 ID 和显示名称，如果未指定显示名称，系统会将桌面 ID 同时用作显示名称。

注释 对于可选描述，您可以使用包括空格在内的任何字母数字字符。描述最多可为 1024 个字符长度，且只能在 View Administrator 中显示。

提供桌面标识的详细信息后，请单击 **[Next （下一步）]**。

6 配置桌面属性，并单击 **[Next （下一步）]**。

警告 如果使用 Windows Vista 虚拟机，则*必须*将电源策略设置为 **[Ensure VM is always powered on （确保虚拟机始终开机）]**。

属性	参数描述
State （状态）	**[Enabled （启用）]** – 创建桌面池后，自动启用桌面池并准备立即使用。 **[Disabled （禁用）]** – 创建桌面池后，即禁用桌面池。如果要执行部署后的活动，如测试或其他形式的基准维护，则该设置很适用。
When VM is not in use （未使用虚拟机时）	**[Do nothing (VM remains on) （不执行任何操作 （虚拟机始终开机））]** – 您可根据需要启动已关机的虚拟机并保持开机状态，即使在不使用时亦如此，直到关机为止。 **[Always on (ensure VM is always powered on) （始终开机 （确保虚拟机始终开机））]** – 池中所有虚拟机始终保持开机，即使在不使用它们时亦如此。如果虚拟机已关机，则系统将立即重新启动该虚拟机。 **[Suspend VM （挂起虚拟机）]** – 不使用时，池中所有虚拟机都处于挂起状态。 **[Power off VM （关闭虚拟机）]** – 不使用时，池中所有虚拟机都将关机。
Automatic logoff after disconnect （断开连接后自动注销）	**[Immediately （立即）]** – 用户在断开连接后立即注销。 **[Never （永不）]** – 永不注销用户。 **[After （之后）]** – 指用户断开连接后，在此时间过后即注销用户。输入持续时间 （以分钟为单位）。
Power off and delete virtual machine after first use （首次使用后关闭并删除虚拟机） （仅限于非永久池）	要在用户注销后立即删除虚拟机，请选择此属性。 如有必要，在删除虚拟机后，可以克隆新虚拟机以维护特定池的大小。

属性	参数描述
Allow users to reset their desktop （允许用户重置桌面）	如果要允许桌面用户在没有管理员协助的情况下重置其桌面，请选择此属性。
Allow multiple sessions per user （允许每个用户多个会话） （仅限于非永久池）	如果要支持各个用户同时连接到同一池中的多个桌面，请选中此属性。
Refresh OS disk on logoff （注销时刷新操作系统磁盘） （仅限于永久池）	**[Never （从不）]** － 从不刷新基础操作系统的映像。 **[Always （始终）]** － 每次注销用户时刷新基础操作系统的映像。 **[Every （间隔时间）]** － 基础操作系统映像在指定时间内定期刷新。请在显示的字段中输入正数天数。 **[At （特定数量）]** － 当操作系统数据量在数据存储中达到一定级别时，刷新基础操作系统映像。请在显示的字段中输入百分比值。
Default display protocol （默认显示协议）	选择您希望 View Connection Server 与 View Client 通信时使用的显示协议。 **PCoIP** － 为 LAN 或 WAN 中的广大用户提供图像、音频和视频内容传送方面的最佳 PC 体验。 PCoIP 可以作为虚拟机和使用 Teradici 主机卡的物理机的单独桌面的显示协议。 **Microsoft RDP** － 一种允许用户连接到运行 Microsoft RDC 的计算机的多通道协议。
Allow users to override the default protocol （允许用户重写默认协议）	如果希望桌面用户可以在 View Client 中重写默认显示协议，请选择此属性。
Max number of monitors （显示器最大数量）	如果使用 PCoIP，请选择用户可用于显示桌面的显示器的最大数量。 **注释：**您必须关闭然后再启动现有虚拟机，才能使该设置生效。
Resolution of each monitor （每台显示器的分辨率）	如果使用 PCoIP，请选择分辨率最高的显示器的像素尺寸。 **注释：**您必须关闭然后再启动现有虚拟机，才能使该设置生效。
Adobe Flash quality （Adobe Flash 质量）	从下拉菜单中，选择 View Client 中显示的 Adobe Flash 动画的质量级别。低的质量级别可在较低带宽的情况下有更快的显示刷新速度。
Adobe Flash throttling （Adobe Flash 调节）	从下拉菜单中，选择 View Client 中显示的 Adobe Flash 动画的调节级别。较高的调节级别，在较低带宽的时候会使动画的帧速率下降。

7 配置桌面部署属性，并单击 **[Next （下一步）]**。

属性	参数描述
Provisioning （部署）	**[Enabled （启用）]**：完成部署步骤或删除桌面后立即在池中创建桌面。 **[Disabled （禁用）]**：完成部署步骤或删除桌面后不立即在池中创建桌面。
Number of desktops （桌面数）	指定要在该池中创建的桌面数。如果选中 **[Advanced Settings（高级设置）]** 面板中的 **[Enable Advanced Pool Settings （启用高级池设置）]** 复选框，则会禁用此设置。

VM naming pattern （虚拟机命名模式）	默认情况下，前缀用来标识属于某一池中相同组的所有桌面。前缀最多为 13 个字符，并附有一个数字后缀，以便将相同池中的每个桌面逐一加以区别。
	通过输入一个包含表示池编号的令牌名称，可以重写此行为，该令牌在任何位置均以相同方式显示。例如：
	`amber-{n}-desktop`
	部署后，系统将使用桌面的池编号替换 `{n}`。
	您可使用 `n:fixed=` 结构输入固定长度的令牌。例如：
	`amber-{n:fixed=3}`
	部署后，系统将使用每个桌面的固定长度池编号替换 `{n:fixed=3}`：`amber-001`、 `amber-002` 和 `amber-003` 等。
	包含令牌且采用固定令牌长度替换的名称最多只能使用 15 个字符。例如：
	`my-view-system{n:fixed=1}`
	其中，令牌长度不固定，其缓冲值为 1，因此，最大 "替换" 长度为 14 个字符。例如：
	`a-view-system{n}`

Stop provisioning on error （出错时停止部署）	如果在创建桌面过程中检测到错误，且需要 View Manager 自动停止部署新虚拟机，请选中此复选框。
Advanced Settings （高级设置）	单击可显示高级池配置设置。通过选中 **[Enable Advanced Pool Settings （启用高级池设置）]** 复选框，可以启用高级参数。此选项将禁用 **[Pool Size （池大小）]** 参数。 **[Number of desktops (minimum) （桌面数量（最小））]**：必须为该池部署的桌面数量的最小值。 **[Number of desktops (maximum) （桌面数量（最大））]**：可为该池部署的桌面数量的最大值。 **[Number of desktops (available) （桌面数量（可用））]**：不需分配的、在任何时候均可使用的虚拟机数。此数字不可超过整个池中的最大可用桌面数。

8 选择要作为部署基础映像的父虚拟机。随后，仅会显示包含在虚拟机关闭时拍摄的一个或多个快照的虚拟机。单击 **[Next （下一步）]**。

9 请选择您先前在父虚拟机处于非活动状态时在其中创建的快照，并单击 **[Next （下一步）]**。

10 选择此桌面池的文件夹要在 vCenter Server 中驻留的位置，并单击 **[Next （下一步）]**。

11 选择要在其中运行此桌面使用的虚拟机的主机或群集。

注释 系统仅支持 8 台或更少主机的群集，并在屏幕中显示。

如果选择了仅包含 ESX/ESXi 4 主机的群集，则 **[Use vSphere mode for View Composer（为 View Composer 应用 vSphere 模式）]** 复选框将变成可用状态。新的 vSphere 模式比之前的版本更加可靠，并支持最新的硬件配置，但是 vSphere 4 要求使用 64 位 (x86_64) 硬件。如果您计划在群集内部署 ESX/ESXi 3.5 主机，请不要选择此复选框。

单击 **[Next （下一步）]**。

12 选择要在其中运行此桌面使用的虚拟机的资源池，并单击 **[Next （下一步）]**。

13 （可选）此步骤仅适用于永久池，它可确定池内的桌面如何存储用户数据。

- 如果在刷新或重构事件后需要保留用户数据，请选中 **[Redirect user profile to a separate disk （将用户配置文件重定向至单独磁盘）]**，并指定用户数据磁盘的最大大小和相关驱动器号。

  如果您使用了多个数据存储，则可以选择 **[Use different datastores for user data disks and OS disks（对用户数据磁盘和操作系统磁盘使用不同的数据存储）]**。然后，在执行步骤 14 选择数据存储时，您可以选择将哪些数据存储用于哪些类型的数据。

警告 请勿选择与父虚拟机中已有驱动器对应的驱动器号。

- 如果不需要在刷新或重构事件后保留用户数据，请选择 **[Store user profile on the same disk as the OS （将用户配置文件存储在操作系统所在的相同磁盘中）]**。在管理员手动执行或系统依据策略自动执行上述任何一种事件后，用户数据就会丢失。

配置用户数据的存储标准之后，请单击 **[Next （下一步）]**。

14 选择一个或多个要在其中存储桌面池的数据存储。如果可用空间不足，则您必须选择额外的数据存储以增加可用空间。

注释 对于群集，仅支持共享数据存储。群集中的每台主机必须连接到要显示的数据存储中。

如果您要创建永久池且在步骤 13 中选择了 **[Use different datastores for user data disks and OS disks （对用户数据磁盘和操作系统磁盘使用不同的数据存储）]** 选项，则可以单击 **[Use For （用于）]** 列中的向下箭头来指定如何使用相应数据存储的存储空间。您可以选择 **[OS Data （操作系统数据）]** 或 **[User Data （用户数据）]**。

注释 您必须为操作系统和用户数据分配足够的空间才可继续。

[Storage Overcommit （存储过载）] 列中的条目将确定系统向数据存储中的可用空间分配新虚拟机的程度。随着存储过载级别的增加，为单个虚拟机增长预留的空间将随之减少，但数据存储中将容纳更多的虚拟机。请单击该条目以修改每个数据存储的过载级别。

注释 [Min Recommended （推荐的最低值）]、 [Storage at 50% provision （50% 部署时的存储）] 和 [Storage at 100% provision （100% 部署时的存储）] 值仅供参考。根据客户端使用模式、应用程序工作负载以及池类型的不同，池的实际要求有所不同。

配置数据存储的存储标准之后，请单击 **[Next （下一步）]**。

15 View Composer 需要使用域用户帐户将链接克隆桌面加入到目标域中。从 **[QuickPrep domain （QuickPrep 域）]** 下拉菜单中，选择域名和用户名条目。您可在第 141 页上的 "在 View Manager 中添加或编辑 vCenter Server 条目" 中所介绍的添加或编辑 vCenter Server 设置的过程中指定这些凭据。

注释 所提供的凭据必须代表一个域帐户 （由 Active Directory 管理员创建），该域帐户有权在指定的 Active Directory 容器中添加和删除计算机对象。请参阅第 130 页上的 "使用 QuickPrep 进行链接克隆桌面部署"。

View Composer 不对您输入的设置进行验证。

如果您希望在关闭桌面之前在其上运行脚本，请在 **[Power-off script （关机脚本）]** 字段中输入父虚拟机上的脚本的路径。

如果您希望在创建、重构或刷新桌面之后在其上运行脚本，请在 **[Post Synchronization script （同步后脚本）]** 字段中输入父虚拟机上的脚本的路径。

输入 Active Directory 容器的相对可区分名称 （例如：`CN=Computers`）。

注释 View Composer 不对您输入的设置进行验证。

单击 **[Next （下一步）]**。

16 随即显示此部署的配置设置摘要。

- 如果您对配置的任何内容不满意，可以使用 **[Back （返回）]** 按钮重新访问先前的任何页面。
- 如果您对配置很满意，请单击 **[Finish （完成）]** 以部署链接克隆桌面池。

启动部署之后，您可以选择 [Desktops （桌面）] 窗格中的 **[Desktops （桌面）]** 选项卡或 **[Desktop Sources （桌面源）]** 选项卡，以监控部署桌面池或单个桌面的过程。

完成此过程之后，您可以执行第 81 页上的 "授权桌面或池" 中所述步骤，向用户或用户组授予使用该桌面池的权利。

刷新、重构和重新平衡链接克隆桌面

您仅可重构、刷新或重新平衡属于永久池组成部分的链接克隆桌面。如果需要更改非永久的链接克隆桌面池的父虚拟机，则必须使用池部署向导直接修改该池。通过在非永久池的 [Summary （摘要）] 页面中单击 **[Edit （编辑）]**，即可调用部署向导。

如果需要在重新平衡之前更改数据存储的部署文件 （即添加或删除存储，或修改池配置），则必须先使用 [Edit Desktop （编辑桌面）] 向导来重新配置该池。

注释 重新平衡将自动启动对目标桌面的刷新。此外，只能重新平衡处于 [Ready （就绪）]、[Error （错误）] 或 [Customizing （自定义）] 状态且未计划取消或等待取消的桌面。

您每次只可以安排一个刷新、重构或重新平衡操作。

警告 在执行本部分所述的任何步骤之前或执行过程中，请勿从 vCenter Server 内修改父虚拟机 （例如，将它转换为模板）。

刷新链接克隆桌面池

1 从 View Administrator 内，单击 **[Desktops and Pools （桌面和池）]** 以显示 [Desktop （桌面）] 页面。

2 请确保已在左侧窗格中选中 **[Inventory （清单）]** 选项卡，并选择要刷新的永久桌面池。

3 选择以下选项之一：

- 要刷新整个桌面池，请确保已在右侧窗格中选中 **[Summary （摘要）]** 选项卡。
- 要刷新桌面池中已分配给特定用户的桌面，请确保已在右侧窗格中选中 **[Users and Groups （用户和用户组）]** 选项卡。

  如果需要刷新一个或多个已分配用户的桌面，请选中对应的复选框。如果需要刷新所有已分配用户的桌面，则不必执行此操作。

- 要刷新池中的特定桌面源，请确保已在右侧窗格内选中 **[Desktop Sources （桌面源）]** 选项卡。

  如果需要刷新多个桌面，请选中对应的复选框。如果需要刷新池中所有桌面，则不必执行此操作。

4 单击 **[Edit Image （编辑映像）]**。随即显示 [Edit Image （编辑映像）] 向导。选中 **[Refresh （刷新）]** 选项，并单击 **[Next （下一步）**。

5 如果已选中 **[Users and Groups （用户和用户组）]** 选项卡，则您现在可以过滤用户选择。如果需要对桌面池中所有已分配的用户执行一次全局刷新，请选中 **[All users （所有用户）]**。如果已选择一个或多个用户，且如果希望仅对所选组内的特定用户应用刷新，则可选择 **[The following users （下列用户）]**。

- 如果已选择 **[Summary （摘要）]** 或 **[Desktop Sources （桌面源）]** 选项卡，则您现在可以过滤桌面源选择。如果需要对池中所有桌面执行一次全局刷新，请选中 **[All virtual machines （所有虚拟机）]**。
- 如果已从 **[Desktop Sources（桌面源）]** 选项卡中指定了一个或多个单独分配的桌面，且如果仅需要对所选组内的特定系统应用刷新，则可选择 **[The following virtual machines （下列虚拟机）]**。

单击 **[Next （下一步）]**。

6 计划要刷新事件的时间 （默认值设置为 [current time （当前时间）]，因此系统将立即刷新）。

- 如果希望启动刷新事件时立即注销任何当前连接的用户，请选中 **[Force Users to log off （强制用户注销）]**。

  注释 如果选中此选项，则系统将在断开连接之前通知已连接的用户，且允许用户有机会关闭应用程序并注销。您可从 [Configuration （配置）] 页面的 **[Global Settings （全局设置）]** 部分内访问此通知消息。

- 如果需要系统等待，直到用户断开连接才启动桌面刷新，请选择 **[Wait for users to log off （等待用户注销）]**。

7 随即显示 [Ready to Complete （准备完成）] 页面。此页面显示刷新任务的摘要信息，其中包括计划的任务开始时间及受影响的虚拟机数量。

8 如果您认为此页面上显示的信息正确，请单击 **[Finish （完成）]** 开始刷新。

重构链接克隆桌面池

1 从 View Administrator 内，单击 **[Desktops and Pools （桌面和池）]** 以显示 [Desktop （桌面）] 页面。

2 请确保已在左侧窗格内选中 **[Inventory （清单）]** 选项卡，并选择要重构的桌面池。

3 选择以下选项之一：

- 要重构整个桌面池，请确保已在右侧窗格中选中 **[Summary （摘要）]** 选项卡。
- 要重构桌面池中已分配给特定用户的桌面，请确保已在右侧窗格中选中 **[Users and Groups （用户和用户组）]** 选项卡。

  如果需要重构一个或多个已分配用户的桌面，请选中对应的复选框。如果需要重构所有已分配用户的桌面，则不必执行此操作。
- 要重构池中的特定桌面源，请确保已在右侧窗格内选中 **[Desktop Sources （桌面源）]** 选项卡。

  如果需要重构多个桌面，请选中对应的复选框。如果需要重构池中所有桌面，则不必执行此操作。

4 单击 **[Edit Image （编辑映像）]**。随即显示 [Edit Image （编辑映像）] 向导。选中 **[Recompose （重构）]** 选项，并单击 **[Next （下一步）]**。

5 如果已选中 **[Users and Groups （用户和用户组）]** 选项卡，则您现在可以过滤用户选择。如果需要对桌面池中所有已分配的用户执行一次全局重构，请选中 **[All users （所有用户）]**。如果已选择一个或多个用户，且如果仅需要对所选组内的特定用户应用重构，则可选择 **[The following users （下列用户）]**。

- 如果已选择 **[Summary （摘要）]** 或 **[Desktop Sources （桌面源）]** 选项卡，则您现在可以过滤桌面源选择。如果需要对池中所有桌面执行一次全局重构，请选中 **[All virtual machines （所有虚拟机）]**。
- 如果已从 **[Desktop Sources （桌面源）]** 选项卡中指定了一个或多个单独分配的桌面，且如果仅需要对所选组内的特定系统应用重构，则可选择 **[The following virtual machines （下列虚拟机）]**。

6 单击 **[Next （下一步）]**。

7 编辑所选桌面池使用的基础映像。

- 如果需要将桌面池中的克隆绑定至同一基础映像内的另一快照中，请从显示的列表中选择一个新快照。
- 如果要将当前基础映像更改为新父虚拟机的基础映像，请单击 **[Change （更改）]**，并从列表中突出显示的虚拟机中选择一个要成为池内主虚拟机的新虚拟机。单击 **[OK （确定）]**。

单击 **[Next （下一步）]**。

8 计划要重构事件的时间（默认值设置为 [current time （当前时间）]，因此系统将立即重构）。

- 如果希望启动重构事件时立即注销任何当前连接的用户，请选中 **[Force Users to log off （强制用户注销）]**。

注释 如果选中此选项，则系统将在断开连接之前通知已连接的用户，且允许用户有机会关闭应用程序并注销。您可从 [Configuration （配置）] 页面的 **[Global Settings （全局设置）]** 部分内访问此通知消息。

- 如果需要系统等待，直到用户断开连接才启动桌面重构，请选择 **[Wait for users to log off （等待用户注销）]**。

9 随即显示 [Ready to Complete （准备完成）] 页面。此页面显示重构任务的摘要信息，其中包括将使用的快照、计划的任务开始时间及受影响的虚拟机数量。

如果您认为此页面上显示的信息正确，请单击 **[Finish （完成）]** 开始重构。

重新平衡链接克隆桌面池

1 从 View Administrator 内，单击 **[Desktops and Pools （桌面和池）]** 以显示 [Desktop （桌面）] 页面。

2 请确保已在左侧窗格内选中 **[Inventory （清单）]** 选项卡，并选择要重新平衡的桌面池。

3 在右侧窗格中，选中 **[Desktop Sources （桌面源）]** 选项卡。

4 从显示的桌面源列表中选择一个或多个桌面。如果要重新平衡整个池，则不必选择任何桌面。

5 单击 **[Rebalance （重新平衡）]**。系统随即显示 [Rebalance （重新平衡）] 向导，它将向您显示相关信息，指出重新平衡池中一个或多个桌面将导致何种结果。如果您已仔细阅读此信息，并希望执行此操作，请单击 **[Next （下一步）]**。

6 如果您先前已从桌面源列表中选择一个或多个虚拟机，则您可通过选中对应的单选按钮来选择仅重新平衡这些系统。如果您尚未选择任何虚拟机，或需要重新平衡整个池，则请选中 **[All virtual machines （所有虚拟机）]**。单击 **[Next （下一步）]**。

7 计划要重新平衡事件的时间（默认值设置为 [current time （当前时间）]，因此系统将立即重新平衡）：

- 如果希望启动重新平衡事件时立即注销任何当前连接的用户，请选中 **[Force Users to log off （强制用户注销）]**。

  注释 如果选中此选项，则系统将在断开连接之前通知已连接的用户，且允许用户有机会关闭应用程序并注销。您可从 View Administrator 中的 [Configuration （配置）] 视图的 **[Global Settings （全局设置）]** 部分内访问此通知消息。

- 如果需要系统等待，直到用户断开连接才启动桌面重新平衡，请选择 **[Wait for users to log off （等待用户注销）]**。

单击 **[Next （下一步）]**。

8 随即显示 [Ready to Complete （准备完成）] 页面。此页面显示重新平衡任务的摘要信息，其中包括计划的任务开始时间及受影响的虚拟机数量。

如果您认为此页面上显示的信息正确，请单击 **[Finish （完成）]** 开始重新平衡。

使用现有 View Composer 数据库

如果在安装 View Composer 服务的过程中选中 ODBC 数据源，则可使用包含 View Composer 数据的现有数据库。但是，为了使该数据源与 View Composer 服务的新实例兼容，必须先将 View Composer 原有服务软件创建的 RSA 密钥容器传输至新的主机系统中。

注释 RSA 密钥对是由 View Composer 服务软件创建的，旨在对 View Composer 数据库内存储的敏感身份验证信息进行加密和解密。

ASP.NET IIS 注册工具随 Microsoft .NET Framework 一起提供，它可支持您执行多种配置操作，其中包括在不同系统之间迁移密钥容器内容。

要执行以下步骤，必须先在包含（或以前包含） View Composer 实例（以前与您要使用的数据库相关联）的系统中安装 .NET Framework。此外，还必须在要安装新实例的系统中安装 .NET Framework。

您可从以下地址下载 .NET Framework，并查看有关 ASP.NET IIS 注册工具的其他信息：

- http://www.microsoft.com/net
- http://msdn.microsoft.com/library/k6h9cz8h(VS.80).aspx

在新系统中安装 View Composer 服务软件之前，您必须执行以下步骤。

在系统之间迁移 RSA 密钥容器

1. 通过在源系统的命令提示符下输入以下内容，可从本地密钥容器中导出与 View Composer 旧实例关联的 RSA 密钥：

   ```
   aspnet_regiis -px "SviKeyContainer" "keys.xml" -pri
   ```

   RSA 公用和专用密钥对将从 SviKeyContainer 容器导出至名为 keys.xml 的文件中，而该文件将保存至本地 ASP.NET IIS 注册工具内。

2. 将 keys.xml 文件复制到需要安装 View Composer 服务软件新实例的系统中。

3. 在目标系统的命令提示符下输入以下内容，将密钥对数据导入到本地密钥容器中，其中 <path> 是指导出文件的路径：

   ```
   aspnet_regiis -pi "SviKeyContainer" "<path>\keys.xml"
   ```

4. 按照第 136 页上的 "向 vCenter Server 添加 View Composer 服务"中所述步骤安装 View Composer 服务，并提供现有数据源的所需信息；不过，在出现提示时，请选择 **[Use the existing RSA key container （使用现有 RSA 密钥容器）]**。

使用 View Composer 的 SviConfig 工具

SviConfig 实用程序与 View Composer 应用程序一起提供，该实用程序使 View Manager 管理员能够升级或还原 View Composer 数据库。

SviConfig 可执行文件的路径是：

```
C:\Program Files\VMware\VMware View Composer\sviconfig.exe
```

本节介绍的命令适用于有经验的 View Composer 管理员，这些命令可以解决与 View Composer 服务相关的问题。

升级 View Composer 数据库 （databaseupgrade）

数据库升级命令用于将 View Composer 1.0 模式升级到 1.1 版。此外，该命令还会将数据库中的信息从 View Composer 1.0 迁移到 View Composer 1.1 中。 View Composer 模式从 1.1 版本起从未发生过变化。

使用情形

在 vCenter Server （已经安装 View Composer 服务的早期版本）中安装 View Composer 服务时，用户可选择手动升级该服务。如果需要升级模式，必须使用 SviConfig 来进行升级并迁移现有数据。

用法

升级 View Composer 数据库之前，必须先关闭 vCenter Server 上运行的 View Composer 服务。成功执行该命令后，请重新启动该服务。

将通过 Windows 命令提示符发出 SviConfig databaseupgrade 命令的指示，其格式如下：

```
sviconfig -operation=databaseupgrade
          -DsnName=<目标数据库源名 (DSN) >
          -Username=<数据库管理员用户名>
          -Password=<数据库管理员密码>
```

例如：

```
sviconfig -operation=databaseupgrade -dsnname=LinkedClone
-username=Admin -password=Pass
```

结果输出

操作成功会产生以下屏幕输出：

```
Establishing database connection.
Database connection established successfully.
Upgrading database.
Load data from SVI_VC_CONFIG_ENTRY table.
Update SVI_DEPLOYMENT_GROUP table.
Update SVI_REPLICA table.
Update SVI_SIM_CLONE table.
SviConfig finished successfully.
Database is upgraded successfully.
```

如果在运行 databaseupgrade 命令时出现错误代码 17，或者在安装 View Composer 服务的过程中显示了以下消息：

Database upgrade completed with warnings（数据库升级已完成，但出现了警告）

请参阅以下 View Composer 日志文件以了解更多信息，然后再（重新）执行 databaseupgrade 命令：

```
C:\Documents and Settings\All Users\Application
Data\VMware\View Composer\Logs\vmware-sviconfig.log
```

结果代码

操作完成时，此工具会返回结果代码。表 6-3 介绍了结果代码。

表 6-3. databaseupgrade 结果代码

代码	描述
0	操作成功结束。
1	找不到所提供的 DSN。
2	提供的数据库管理员凭据无效。
3	此数据库的这个驱动程序不受支持。
4	出现异常问题，命令无法完成。
14	另一个应用程序正在使用 View Composer 服务。执行命令前，请关闭该服务。
15	还原进程中出现问题，其详细信息作为屏幕日志输出的一部分提供。
17	无法升级数据库数据。
18	无法连接到数据库服务器。

还原 View Composer 数据库 （restoredata）

可以将 View Connection Server 设置为创建 View LDAP 和 View Composer 数据库数据的手动或自动备份。使用 `restoredata` 命令，可将与 View Composer 部署相关的备份文件导入到存储链接克隆信息的 SQL 数据库中，以便将您的 View 环境还原到早期状态。

注释 有关如何手动或自动创建备份文件的信息，请参阅第 55 页上的 "View Server"。

默认情况下， View Connection Server 上的备份文件存储在以下位置：

```
C:\Documents and Settings\All Users\Application
Data\VMware\VDM\backups
```

View Composer 备份文件使用以下命名习惯：

```
Backup-<年><月><日><计数>-<vCenter Server 服务器名>
_<域名>.SVI
```

例如：

```
Backup-20090304000010-foobar_test_org.SVI
```

使用情形

出现系统故障后需要复制或还原 View Composer 数据库数据时，或者希望将 View Composer 部署恢复到早期状态时，请使用此命令。

用法

导入备份数据之前，必须先关闭 vCenter Server 上运行的 View Composer 服务。成功执行该命令后，请重新启动该服务。

将通过 Windows 命令提示符发出 SviConfig `restoredata` 命令的指示，其格式如下：

```
sviconfig -operation=restoredata
          -DsnName=< 目标数据库源名 （DSN） >
          -Username=< 数据库管理员用户名 >
          -Password=< 数据库管理员密码 >
          -BackupFilePath=<View Composer 备份文件的路径 >
```

例如：

```
sviconfig -operation=restoredata -dsnname=LinkedClone -username=Admin
-password=Pass -backupfilepath="C:\Program Files\VMware\VMware View
Composer\Backup-20090304000010-foobar_test_org.SVI"
```

结果代码

操作完成时，此工具会返回结果代码。表 6-4 介绍了结果代码。

表 6-4. restoredata 结果代码

代码	描述
0	操作成功结束。
1	找不到所提供的 DSN。
2	提供的数据库管理员凭据无效。
3	此数据库的这个驱动程序不受支持。
4	出现异常问题，命令无法完成。
14	另一个应用程序正在使用 View Composer 服务。执行命令前，请关闭该服务。
15	还原进程中出现问题，其详细信息作为屏幕日志输出的一部分提供。

Offline Desktop

7

使用 Offline Desktop，移动用户可将特定类型的 View Manager 桌面的克隆实例检出到本地系统（如笔记本电脑）中。检出后，本地副本相当于一个独立的桌面系统，无论连网与否均可使用；检出后，该桌面就被视为"脱机桌面"。

以下内容将概述 Offline Desktop 及其用途和实施情况。

注释 Offline Desktop 是一种试验性功能。有关试验性功能的详细信息，请参阅第 14 页上的"系统要求"。

vSphere 4 不支持 Offline Desktop。

本章讲述以下主题：

注释 有关脱机客户端会话特有的使用策略信息，请参阅第 173 页上的"客户端策略"。

Offline Desktop 概述

Offline Desktop 可解决任何联机桌面解决方案中都含有的持续访问难题：根据具体情况或用户选择，用户经常发现自己面临着网络可用性极其受限、或根本无法连网的状况。

面对这种情况， Offline Desktop 用户可以使用 View Client with Offline Desktop 应用程序从 View Connection Server 中下载桌面虚拟机副本，以便在本地计算机中使用。此操作还会导致 "锁定" 联机桌面虚拟机，防止从任何其他位置访问该虚拟机。

注释 锁定后，将禁用 vCenter Server 操作，如启动联机桌面、拍摄快照、编辑虚拟机设置等。

下载后，脱机桌面的行为方式与联机桌面相同，仍可充分利用本地资源，最大程度地减少滞后时间，同时显著增强性能。下载的虚拟机不会影响客户系统的现有操作系统，用户仍可根据需要继续利用它们。

针对联机会话和脱机会话使用带 Offline Desktop 的 View Client，可确保用户体验一致。此外，用户还可与脱机桌面断开连接，然后在不连接到 View Connection Server 的情况下再次登录。恢复网络访问后 （或当用户就绪时）， 您可针对检出的虚拟机采取以下操作：

- 备份 － 使用所有新数据和配置来更新联机系统，但脱机桌面在本地系统中仍保持检出状态，且仍保持联机锁定。
- 回滚 － 放弃脱机桌面，并解除联机锁定。以后的客户端连接会定向到联机系统，直到再次检出桌面。
- 检入 － 将脱机桌面上传到联机主机，并解除联机锁定。以后的客户端连接会定向到联机系统，直到再次检出桌面。

注释 执行以上操作时，用户无法访问脱机桌面。

只能通过授权和 Offline Desktop 访问策略，让用户下载联机桌面在本地系统中使用。检出桌面后， View Manager 管理员仍可以在监控脱机桌面的同时访问联机系统。

图 7-1 中展示了联机和脱机一般使用情况的流程，表 7-1 对每个阶段进行了汇总。

图 7-1. Offline Desktop – 使用流程

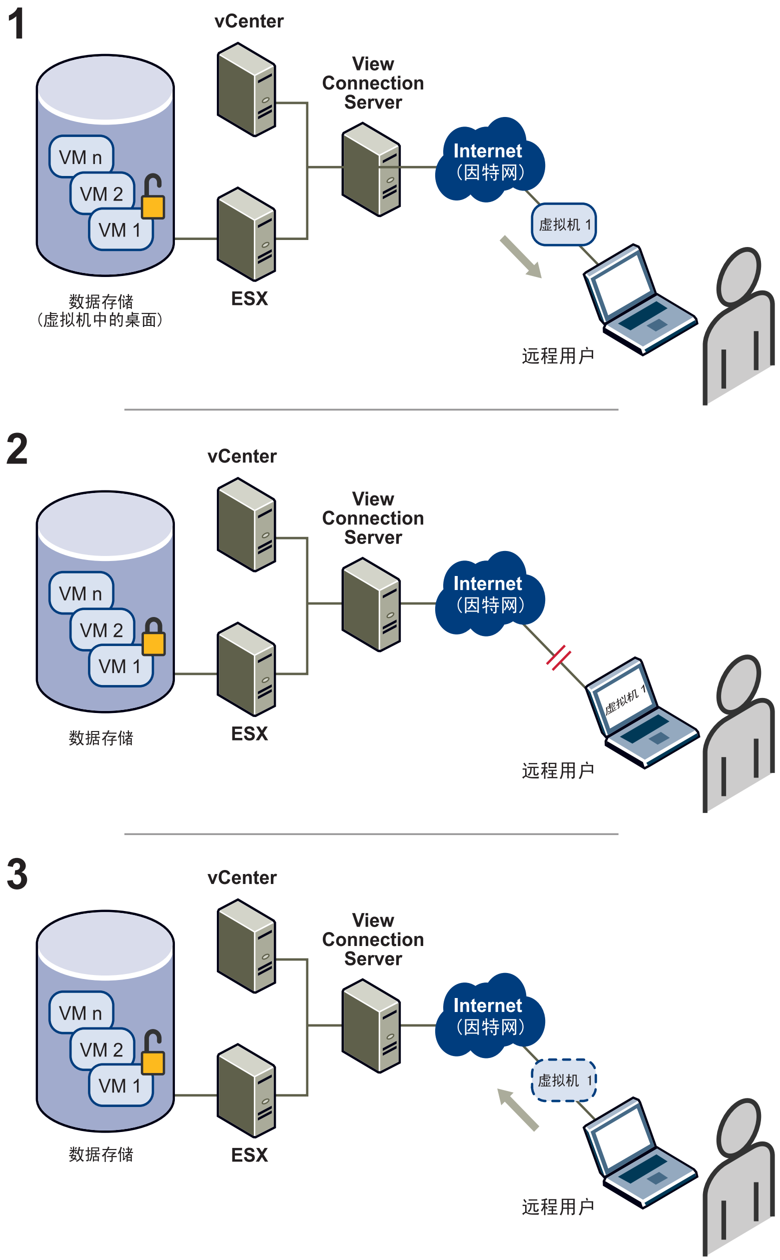


表 7-1. Offline Desktop – 阶段描述

阶段	描述
1	远程用户启动 View Client with Offline Desktop，系统随即向用户列出已授权的桌面。 用户选择 Offline Desktop 兼容桌面并开始下载，将桌面虚拟机复制到本地系统中。
2	成功下载虚拟机后，用户可以登录到 Windows 在本地使用桌面，即使在未连接网络的情况下也可以。 将关闭并锁定对应的联机桌面，防止访问或修改。 在本地工作时，用户可以随时将数据备份到服务器。
3	用户将虚拟机重新检入到服务器时，系统会更新联机数据并解除服务器锁定。 View Client with Offline Desktop 的后续连接将定向到联机桌面，直到再次检出虚拟机。

Offline Desktop 许可和 vCenter Server 访问权限

Offline Desktop 功能的可用性由 View Connection Server 许可证类型决定。要使用 Offline Desktop 相关的管理组件和客户端组件，许可证必须包含 Offline Desktop 功能。

注释 通过查看 View Administrator 的 **[Configuration （配置）]** 视图中的 [License （许可证）] 部分，可以检查 Offline Desktop 许可证的状态。

仅当 View Manager 中指定的 vCenter Server 用户为管理员时，才能从 vCenter Server 中检出桌面。尝试使用 Offline Desktop 之前，请确保 vCenter Server 用户拥有管理权限。

注释 通过查看 View Administrator 的 **[Configuration （配置）]** 视图中的 [vCenter Server] 框，可以检查当前分配给 View Manager 的 vCenter Server 用户。

存储、通信和安全性

初次检出桌面时，由于必须先将整个虚拟机克隆下载到客户系统中，因此所需时间明显长于后续检入和检出所需的时间。此外，由于服务器和客户端之间存在差异，因此这两个系统之间的增量更改也会通信，这一过程还会涉及到传输较小的数据卷。

检出后， Offline Desktop 会使用精简部署的虚拟磁盘将信息存储在主机系统中。这类磁盘占用的空间不会超过其中数据所需的空间，并且仅随着数据的写入来分配物理磁盘空间，从而最大程度地减少下载系统所占用的存储内存空间。

如果客户系统已连网，则检出的桌面将继续与 View Connection Server 进行通信，以便获得使用情况数据、提供策略更新，并确保本地缓存的身份验证标准为最新标准。系统每隔 5 分钟会尝试一次连接。如果没有连网，则桌面将使用本地缓存的信息，以便在登录过程中对用户进行身份验证。

每个脱机系统中的数据均已加密，且其生命周期通过策略加以控制。如果客户端与 View Connection Server 失去连接，则断开连接的最长时间是指用户被拒绝访问之前可以继续使用桌面的时间长度。一旦重新建立连接，就会重置此倒计时。在断开连接之前，系统将通知用户脱机桌面的生命周期即将到期。

同样，如果删除用户访问权限 （即撤消授权或挂起帐户），则在缓存过期时或客户端通过 View Connection Server 知晓此变更之后（以二者中首先发生的事件为准），客户系统将无法访问。在此情况下，断开连接前不会向用户发出通知。

安全加密链路通信和 SSL

对于基于 LAN 的数据传输，Offline Desktop 支持安全加密链路通信或非安全加密链路通信。

- 启用安全加密链路时，所有流量均通过 View Connection Server 进行传送。
- 未启用安全加密链路时，直接在联机桌面主机系统与脱机客户端之间传输数据。

通过在管理界面的 **[Configuration （配置）]** 页面中选中 **[Direct connection for Offline Desktop operations（Offline Desktop 操作采用直接连接）]** 复选框，可以禁用安全加密链路。

除了指定通信路由以外，您还可以通过在管理界面的 **[Configuration （配置）]** 页面中选中 **[Require SSL for Offline Desktop operations （Offline Desktop 操作要求使用 SSL）]** 复选框，对 Offline Desktop 客户端与 View Connection Server 之间的通信和数据传输进行加密。

注释 如果绕过安全加密链路并采用未加密的连接，则会提高数据传输速度，但会损害安全数据通信。加密设置对脱机数据本身并无影响，脱机数据始终都是在客户系统中加密的。

Offline Desktop 策略

您可通过策略控制某些 Offline Desktop 功能。有关在全局级别、池级别或用户级别中配置策略并将其应用到脱机桌面的更多信息，请参阅第 173 页上的 “客户端策略”。

受支持的桌面类型

并非所有类型的 View Manager 桌面配置都支持 Offline Desktop。表 7-2 中列出了此功能对不同桌面类型的可用性。

表 7-2. Offline Desktop – 受支持的桌面

类型	永久性	桌面配置	Offline Desktop
Individual Desktop（单个桌面）	Non-persistent（非永久）	由 vCenter Server 管理的虚拟机	是
		不由 vCenter Server 管理的虚拟机	否
		物理系统	
Automated Desktop Pool（自动桌面池）	Persistent（永久）	非链接克隆	是
		链接克隆	否
	Non-persistent（非永久）	所有	
Manual Desktop Pool （手动桌面池）	Persistent（永久）	由 vCenter Server 管理的虚拟机	是
		不由 vCenter Server 管理的虚拟机	否
		物理系统	
	Non-persistent（非永久）	所有	
Microsoft Terminal Services Desktop Pool（Microsoft 终端服务桌面池）	不适用	不适用	

其他注意事项

使用 Offline Desktop 时，必须注意以下事项：

- View Client with Offline Desktop 无法在虚拟机中运行。
- View Client with Offline Desktop 不支持使用智能卡。
- 您无法将桌面下载到客户机功能优于主机功能的系统中。主机系统的功能至少应与客户机功能相当，才能运行 View Manager 桌面。
- 如果其他用户当前已登录到桌面，则您无法下载此桌面。
- ESX 支持同时检出两个桌面。 ESXi 支持同时检出五个桌面。

- 不支持主机 CD-ROM 重定向。
- 检出桌面后，NAT 用于网络通信。脱机系统的 MAC 地址与相应联机系统的 MAC 地址相同。
- 使用 RDP，您可以在主机与客户机系统之间复制和粘贴文本。但是，您无法在系统之间复制和粘贴系统对象，如文件夹和文件。
- 本地驱动器自动装载至客户机系统中。
- 在客户系统上检出某个桌面后，在 View Administrator 中对桌面或桌面池设置所做的任何更改，只有再次检入该桌面后才能应用到该桌面。

安装并运行 View Client with Offline Desktop

要访问脱机桌面，用户必须先使用 View Client with Offline Desktop 应用程序将联机虚拟机的副本下载到本地系统。在已安装以下应用程序的任何系统中，均不能安装 View Client with Offline Desktop：

- VMware Workstation
- VMware ACE
- VMware Player
- VMware Server

在安装 View Client with Offline Desktop 之前，必须卸载上述应用程序。

注释 View Client 应用程序可提供由 View Client with Offline Desktop 提供的部分功能。但是，这两个应用程序的许多管理任务和连接注意事项都相同，其中包括通过命令提示符启动应用程序时可以调用的许多启动选项。有关此操作的详细信息，请参阅第 89 页上的第 5 章，“客户端管理”。

在首次下载自动池桌面之前，用户必须使用任何 View Manager 客户端连接到此桌面。这样可确保在该桌面中创建一个本地配置文件。使用此文件，可在无法连网时对脱机会话进行身份验证。此外，还可确保桌面与 View Manager 中的用户正确关联。对于单个桌面，此步骤是可选步骤（但建议执行）。

注释 在可以连网的环境中，始终由 View Connection Server 对用户会话进行身份验证。

安装 View Client with Offline Desktop

1 在要安装客户端的系统中运行 View Client with Offline Desktop 可执行文件，其中 xxx 指文件的内部版本号：

```
VMware-viewclientwithoffline-xxx.exe
```

2 显示 VMware 安装向导时，请单击 **[Next （下一步）]**。

3 接受 VMware 许可条款并单击 **[Next （下一步）]**。

4 选择自定义的安装选项：

- 如果不希望用户通过其桌面访问本地连接的 USB 设备，请取消选择 **[USB Redirection （USB 重定向）]** 组件。
- 如果希望所有的用户提供识别和凭据信息以登录到 View Connection Server 并访问 View 桌面，请取消选择 **[Log in as current user （作为当前用户登录）]** 组件。

  注释 Windows XP Home、 Windows Vista Home Basic、 Windows Vista Home Premium 和 Windows 2000 不支持 [Log in as current user （作为当前用户登录）] 功能。

- 您必须安装 **View Client with Offline Desktop** 组件，才能使用 Offline Desktop 功能。

5 如果选择了 **[Log in as current user（作为当前用户登录）]** 组件，您可以进一步配置用户通过 View Client 登录时的默认行为：

- 选择 **[Show in connection dialog （显示在 "连接" 对话框内）]**，可以在 View Client 连接对话框中显示 **[Log in as current user（作为当前用户登录）]** 复选框。

  当选择了该复选框时，用户在登录客户端系统时提供的身份和凭据信息会传送到 View Connection Server 实例，最后传送到 View 桌面。

- 选择 **[Set default option to login as current user （设置默认选项，作为当前用户登录）]** 可默认选择 View Client 连接对话框中的 **[Log in as current user （作为当前用户登录）]** 复选框。

单击 **[Next （下一步）]**。

6 接受默认的目标文件夹或单击 **[Change （更改）]** 以使用其他的目标文件夹，然后单击 **[Next （下一步）]**。

7 （可选）输入客户端要连接的服务器的默认 IP 地址或 FQDN，然后单击 **[Next （下一步）]**。

8 配置 View Client 的快捷方式，然后单击 **[Next （下一步）]**。

9 安装完成后，要启动 View Client，请选中此复选框。

10 单击 **[Install （安装）]** > **[Finish （完成）]**。

启动 View Client with Offline Desktop

1 如果 View Client 在安装完成后没有自动启动，请双击桌面快捷方式或单击 **[Start （开始）]** > **[Programs （程序）]** > **[VMware]** > **[View Manager Client]**。

2 在 **[Connection Server （连接服务器）]** 下拉菜单中，输入 View Connection Server 的主机名或 IP 地址。

3 （可选）如果显示了 **[Log in as current user （作为当前用户登录）]** 复选框，您可以选中该复选框，以使用您在登录该系统时指定的凭据来登录 View Connection Server 和 View 桌面。

   如果未选择 **[Log in as current user （作为当前用户登录）]**，则需要多次提供凭据进行登录，才能访问 View 桌面。

   如果选择了 **[Log in as current user （作为当前用户登录）]**，并且有权登录 View Connection Server，则系统不会提示您输入步骤 5 中的登录凭据。

4 单击 **[Connect （连接）]**。

5 输入已授权的用户凭据，选择域，然后单击 **[Login （登录）]**。

   如果输入的用户名格式为 `user@domain`，该用户名将因为带有 @ 符号而被视作用户主体名称 (UPN)。因此域下拉菜单将会灰显。

6 从提供的列表中选择桌面，并单击 **[Connect （连接）]**。

   View Client 将尝试连接到指定的桌面。

连接成功后，屏幕上将显示客户端窗口。

在 View Client with Offline Desktop 提供的列表中右键单击桌面，显示其上下文菜单，用户可确定该桌面是否可以检出。如果桌面可以脱机使用，则会显示 **[Check out （检出）]** 选项。

注释 只有检出桌面的用户才能访问该桌面，即使桌面已授权给某一用户组也是如此。

检出桌面

首次检出桌面时，用户可以指定下载的虚拟机将存放在本地系统中的位置。检出操作开始后，屏幕指示器将显示下载进度。

注释 在联机与脱机环境之间移动数据时，用户右键单击某个条目即可显示其上下文菜单，可在其中暂停或取消检入或检出进程。

下载数据之后，用户访问将定向到脱机桌面，直到将其重新检入。

注释 如果用户将系统中的虚拟机数据手动移到备用位置或其他系统中，则用户无法使用其脱机桌面。

Offline Desktop 状态

通过单击 **[Desktops and Pools （桌面和池）]** 按钮，然后选择 **[Offline Sessions （脱机会话）]** 选项卡，您可以为 View Administrator 中的所有桌面或特定池检查全局级别或桌面池级别中当前的所有脱机会话。

此视图将向您显示一个窗格，其中包含一个状态表，表中已列出该服务器当前已知的所有脱机会话。表 7-3 中描述了此表的列条目。

表 7-3. 脱机会话

字段	描述
User （用户）	已检出桌面的用户的 Active Directory ID。此 ID 的格式为 **domain\username**，也可以为 **username@domain** （对应给出用户主体名称 （User Principal Name， UPN）的情况）。
Desktop （桌面）	永久池或桌面池的显示名称 （如果在 View Manager 中创建桌面或池时提供了显示名称）。
Status （状态）	当前的检出状态，可为以下状态之一： ■ [Checking out （正在检出）] – 正在将数据下载到客户系统，或在传输过程中已暂停下载 ■ [Checked out （已检出）] – 脱机桌面已位于客户系统中，对应的联机桌面已锁定 ■ [Checking in （正在检入）] – 正在从客户系统中上传数据 （无论是以备份形式、还是完全检入形式），或在传输过程中已暂停上传
Check-out Time （检出时间）	客户端上次启动检出的时间。
Offline Duration （脱机持续时间）	自检出桌面之后 View Connection Server 已知的脱机使用总时间。

表 7-3. 脱机会话 （续）

字段	描述
Last Server Contact （上次服务器连接）	View Client with Offline Desktop 上次连接到 View Connection Server 的时间。允许建立连接时，每隔 5 分钟会连接一次服务器。
Last Backup （上次备份）	脱机桌面上次备份到 View Connection Server 的时间。如果尚未进行备份，则所示时间与 **[Check-out Time （检出时间）]** 相同。

除了可以查看上述信息以外，通过从列表中选择桌面并单击 **[Details （详细信息）]**，您还可以查看客户系统的主机名和 IP 地址、已检出桌面的名称及其 DNS 条目或 IP 地址。

客户端连接

您可以授权多个用户使用一个系统，但只有最初检出桌面的用户才可使用 View Client with Offline Desktop 应用程序本地访问该桌面。

如果用户在网络断开的情况下连接到脱机桌面，则系统将使用本地缓存的用户信息对用户进行身份验证。登录后，如果已恢复网络连接，则用户必须重新进行身份验证才能继续使用该桌面；如果已启用 RSA 身份验证，则同样需要此信息。

删除访问权限

除了 Active Directory 提供的挂起或删除帐户这一标准方法以外，通过从单个桌面或桌面池中删除用户授权、或放弃脱机会话，还可以从管理界面中终止 Offline Desktop 会话。

如果从包含处于活动状态的、且已检出会话 （其中的 View Connection Server 可以与客户端进行通信）的单个桌面或桌面池中删除授权，则只要客户端检测到授权已撤消，桌面将会立即挂起。挂起后，系统将向用户显示错误，通知用户不再允许桌面脱机运行。

如果无法与脱机客户端建立通信，则系统将通知用户：下次尝试在连网情况下访问桌面时，会删除用户访问权限。

回滚桌面

此外，您还可以通过回滚脱机会话删除客户端对脱机桌面的访问权限。启动回滚事件后，系统将通知脱机客户端 （如果能够连接该客户端），不再允许该用户登录到已检出的桌面。

- 如果在用户登录时已回滚检出的桌面，则当前会话将在 View Client with Offline Desktop 收到通知后立即终止。
- 如果用户尚未登录，则后续连接尝试将重定向到联机桌面。

要继续使用脱机桌面，用户必须立即从服务器中检出桌面。

要回滚脱机桌面会话，请从 **[Offline Sessions （脱机会话）]** 选项卡下的表中提供的列表内选择该桌面，并单击 **[Rollback （回滚）]**。

如果客户端策略允许，则用户还可以通过右键单击脱机桌面条目、并从上下文菜单中单击 **[Rollback （回滚）]**，从 View Client 或 View Portal 桌面中回滚桌面。只有检出该桌面的用户才能执行以上操作。

注释 在任何处于活动状态的传输过程中，均无法执行回滚操作。

组件策略

8

策略是指系统管理员定义的用来控制应用程序行为的一项或一套规则。在 View Manager 内，可通过各种策略建立所含组件的配置，方法包括控制信息记录、管理客户端的访问、限制设备的使用、针对客户端的使用建立安全性参数，等等。

有些组件策略可以通过 View Administrator 进行分配，而其他组件策略包含在 Active Directory 中的组策略对象内，并在 Windows 注册表级别应用于用户或桌面。以下内容将详细介绍每种策略的用途及其配置位置和应用范围。

本章讲述以下主题：

电源策略

在部署过程中，您可通过多种桌面或桌面池为桌面源配置电源策略。电源策略可控制桌面在不使用时的行为方式，因此，该策略是在 View Manager 环境中管理资源的重要机制。

注释 在用户登录之前、断开连接或注销之后， View Manager 桌面都不在使用中。

表 8-1 描述了可在部署过程中分配给桌面或桌面池的各种虚拟机电源策略状态。

表 8-1. 电源策略定义

属性	描述
Do nothing (VM remains on)（不执行任何操作 （虚拟机始终开机））	您可根据需要启动已关闭的虚拟机并保持打开状态，即使在不使用时亦如此，直到关机为止。
Always on （ensure VM is always powered on）（始终开机 （确保虚拟机始终开机））	池中所有虚拟机均始终启动，即使在不使用时亦如此。如果虚拟机已关机，则系统将立即重新启动该虚拟机。
Suspend VM （挂起虚拟机）	不使用时，池中所有虚拟机都将处于挂起状态。
Power off VM （关闭虚拟机）	池中所有虚拟机会在用户注销后关机，但不会在用户断开连接后关机。

表 8-2 描述了应用电源策略的情况。

表 8-2. 电源策略说明

桌面类型	将应用电源策略的情况……
单个桌面（由 vCenter Server 管理的虚拟机）	用户断开连接或注销之后。
永久自动池	在不使用时，或在用户断开连接或注销之后。此策略仅适用于未分配的桌面。
非永久自动池	在不使用时，或在用户断开连接或注销之后。 **注释：**如果在断开连接之后应用 **[Power Off （关闭）]** 策略，则系统将放弃会话。如果在断开连接之后应用 **[Suspend （挂起）]** 策略，则系统可能会创建单独的会话 （桌面为非永久桌面，因此无法保证用户能够返回至该桌面）。 要防止以上任一种情况，请确保将 **[Automatic logoff after disconnect （断开连接后自动注销）]** 设置为 **[Immediately （立即）]**。
永久手动池 （由 vCenter Server 管理的虚拟机）	用户断开连接或注销之后。此策略仅适用于未分配的桌面。

表 8-2. 电源策略说明 （续）

桌面类型	将应用电源策略的情况……
非永久手动池	用户断开连接或注销之后。 **注释：**如果在断开连接之后应用 **[Power Off （关闭）]** 策略，则系统将放弃会话。如果在断开连接之后应用 **[Suspend （挂起）]** 策略，则系统可能会创建单独的会话（桌面为非永久桌面，因此无法保证用户能够返回至该桌面）。 要防止以上任一种情况，请确保将 **[Automatic logoff after disconnect （断开连接后自动注销）]** 设置为 **[Immediately （立即）]**。
物理系统 / 终端服务桌面池	不适用

自动池中的电源策略

在自动池中，默认情况下将电源策略作为与桌面可用性相关的规则。可用桌面是指处于活动状态的、不包含任何用户会话、未分配给用户、且包含一个处于活动状态的 View Agent 服务软件的桌面， View Agent 服务软件可以根据以上标准确认 View Connection Server 是否可以使用该桌面。

电源策略示例 1

如果要求特定数量的桌面随时可用，则这些桌面的电源策略必须确保这些桌面始终启动。下列池示例中说明了此行为，表 8-3 中提供了相应参数。

表 8-3. 池示例 1

类型	最小数	最大数	可用数	电源策略
非永久自动池	10	20	2	Suspend VM（挂起虚拟机）

部署过程完成后，系统将创建 10 个桌面：其中 2 个桌面已启动且立即可用，其余 8 个处于挂起状态。对于连接的每个新用户，系统均会启动一个桌面，以便维护可用性级别。

当连接用户数超过 8 时，系统将额外创建一个桌面 （最多不超过 20 个），以便维护可用性级别。达到桌面最大数之后，要断开连接的前 2 名用户的桌面始终保持启动，以便维护可用性阈值。根据策略，系统将暂停要断开连接的每个后续用户的桌面。

电源策略示例 2

在下列池示例 （表 8-4 中提供了相应参数）中，最大桌面数和最小桌面数相同。

表 8-4. 池示例 2

类型	最小数	最大数	可用数	电源策略
非永久自动池	5	5	2	Suspend VM （挂起虚拟机）

最初，系统将创建 5 个桌面：其中 3 个将挂起，其余 2 个均已启动并立即可用。如果此池中的第四个桌面系统挂起，则系统会因已达到最大桌面数而不创建其他桌面。相反，将恢复现有的其中一个系统。

电源策略示例 3

永久自动池的行为略有不同。尽管桌面可能已启动，但由于它可能已分配给用户，因此不得将其视为可用桌面。表 8-5 中描述了此类池的参数示例。

表 8-5. 池示例 3

类型	最小数	最大数	可用数	电源策略
永久自动池	3	5	2	Always on（ensure VM is always powered on）（始终开机 （确保虚拟机始终开机））

在此示例中，您已创建并启动 3 个桌面。如果稍后在 vCenter Server 中手动关闭桌面，则系统将根据策略立即重新启动这些桌面。

一旦用户连接到某一桌面，该桌面将永久分配给该用户。该用户断开连接之后，任何其他用户均无法再使用此桌面。如果从 vCenter Server 中关闭已分配的桌面，虽然已分配的 View Manager 用户的重新连接将再次自动启动桌面，但桌面仍会保持关闭状态（电源策略不再适用）。

此时，池中仍然存在足够多的未分配的桌面，它们可以满足可用性标准。但是，当另一用户连接时，第二个桌面将变为已分配状态。现在，可用桌面数已低于阈值级别，因此，系统将创建并启动新桌面。

在上述情况下，每次分配新用户时，系统都会额外创建一个桌面，直到达到最大桌面阈值为止。

客户端策略

使用 View Administrator 中 [Policies （策略）] 选项卡下的属性，您可控制全局级别、桌面池级别或桌面用户级别中的客户端组件行为。默认情况下，每个用户级别策略都将继承池级别策略中的设置，而池级别策略又继承全局策略中的设置。

您可直接从 View Administrator 内配置许多与桌面会话相关的常规组件行为。这些行为策略既适用于 View Client、又适用于 View Client with Offline Desktop。表 8-6 描述了这些策略。

表 8-6. 客户端策略

属性	描述
USB Access （USB 访问）	指定桌面是否可以使用 USB 设备连接到客户系统。作为一项安全性措施，管理员可阻止使用外部设备。 可用选项包括 **[Allow （允许）]** 和 **[Deny （拒绝）]**。池级别策略和用户级别策略还可从相应的父策略中**继承**默认设置。 默认设置为 [Allow （允许）]。
MMR	指定是否在客户端中启用多媒体重定向 （MMR）。 MMR 是指一种直接通过 TCP 套接字将多媒体数据从远程桌面中的特定编解码器转发至客户端的 Microsoft DirectShow Filter。转发后，数据直接在播放数据的客户端中进行解码。 如果客户端资源不足，无法处理本地多媒体解码，则管理员可禁用 MMR。 可用选项包括 **[Allow （允许）]** 和 **[Deny （拒绝）]**。池级别策略和用户级别策略还可从相应的父策略中**继承**默认设置。 **注释：**如果客户端视频显示硬件不支持覆盖功能， MMR 将无法正常运行。MMR 策略不适用于 Offline Desktop 会话。 默认设置为 [Allow （允许）]。

表 8-7 描述了专门与 Offline Desktop 会话相关的 View Manager 策略。

表 8-7. Offline Desktop 的客户端策略

属性	描述
Offline Desktop	指定是否可以检出桌面供本地使用。 可用选项包括 **[Allow （允许）]** 和 **[Deny （拒绝）]**。池级别策略和用户级别策略还可从相应的父策略中**继承**默认设置。 默认设置为 [Allow （允许）]。
User-initiated Rollback （用户启动回滚）	指定是否允许用户为恢复使用联机版本而放弃脱机桌面。执行此操作时，系统将解除联机桌面的锁定，并放弃脱机桌面。稍后，如有必要，您可手动删除包含脱机桌面数据的本地文件夹。 可用选项包括 **[Allow （允许）]** 和 **[Deny （拒绝）]**。池级别策略和用户级别策略还可从相应的父策略中**继承**默认设置。 默认设置为 [Allow （允许）]。
Max time without server contact （未连接服务器的最长时间）	指定 Offline Desktop 桌面在未成功连接 View Connection Server 进行策略更新的情况下可以运行的时间长度。达到此时间限制时，系统将向用户显示警告，并挂起脱机桌面。 池级别策略和用户级别策略的可用选项包括 **[Inherit （继承）]**（其中，默认设置是从父策略中继承的）和 **[Set （设置）]**。 选中 **[Set （设置）]** 时，您稍后可在显示的字段中以 **[Days （天数）]**、**[Hours （小时）]** 或 **[Minutes （分钟）]** 为单位输入缓存的生命周期。 您可采用相同方式在全局级别中修改此策略，首先应修改 **7** 天这一默认值。

配置和应用客户端策略

如果新的池级别策略更加严格苛刻，则可对池级别策略进行配置，以便重写等效的全局策略。

例如，如果桌面检出的全局策略为 **[Allow （允许）]**，则您可以将等效的池级别策略设置为 **[Deny （拒绝）]**。但反过来并非如此。如果桌面检出的全局策略为 **[Deny （拒绝）]**，则您不能对等效的池级别策略应用 **[Allow （允许）]**。

同样，如果将全局策略 （指定已检出桌面在未成功连接服务器的情况下可以运行的时间长度）设置为 10 分钟，则您不能对任何桌面池应用 30 分钟的服务器连接策略。

注释 如果您尝试在池中应用限制相对较少的策略，则 View Administrator 将向您发出警告。

用户级别策略可重写全局级别策略或池级别策略，即这些策略的限制性可高、可低。例如，如果所有检出桌面的全局服务器连接策略为 10 分钟，且池级别的等效策略为 5 分钟，则您可将 30 分钟的服务器连接策略分配给该池中的任何用户。

配置和分配全局策略设置

1 从 View Administrator 内单击 **[Desktops and Pools （桌面和池）]** 按钮 （）以显示 [Global desktop and pool view （全局桌面和池视图）]，然后单击 **[Inventory （清单）]** 选项卡。在 **[Inventory （清单）]** 窗格中，请确保已选中顶层的 **[Desktops （桌面）]** 条目 （）。

2 在 [Desktops （桌面）] 窗格中，单击 **[Global Policies （全局策略）]** 选项卡。随即显示 [Global policies （全局策略）] 页面。

3 在 [View Policies（视图策略）] 框或 [Offline Desktop Policies（脱机桌面策略）] 框中，单击 **[Edit （编辑）]**。随即显示相应的策略窗口。

注释 检入桌面之前，虚拟桌面的电源策略不会生效。

4 指定策略设置，并单击 **[OK （确定）]**。现在，已应用全局策略设置。

配置和分配池级别的策略设置

1 从 View Administrator 内单击 **[Desktops and Pools （桌面和池）]** 按钮 （）以显示 [Global desktop and pool view （全局桌面和池视图）]，然后单击 **[Inventory （清单）]** 选项卡。

2 在 **[Inventory （清单）]** 窗格中，选择与要应用策略的池对应的桌面池条目 （）。

3 在 [Desktops （桌面）] 窗格中，单击 **[Policies （策略）]** 选项卡。随即显示此桌面池的策略页面。

4 在 [View Policies（视图策略）] 框中，单击 **[Edit Pool Policies（编辑池策略）]**。如果您已选中一个脱机桌面，并要配置脱机策略，请单击 **[Offline Desktop Policies （脱机桌面策略）]**。随即显示相应的策略窗口。

5 指定 **[Offline Desktop （脱机桌面）]**、 **[User-initiated rollback （用户启动回滚）]** 和 **[Max time without server contact （未连接服务器的最长时间）]** 策略设置，并单击 **[OK （确定）]**。现在，已应用池级别的策略设置。

配置和分配用户级别的策略设置

1 从 View Administrator 内单击 **[Desktops and Pools （桌面和池）]** 按钮 （）以显示 [Global desktop and pool view （全局桌面和池视图）]，然后单击 **[Inventory （清单）]** 选项卡。

2 在 **[Inventory （清单）]** 窗格中，选择与要应用策略的池对应的桌面池条目 （）。

3 在 [Desktops （桌面）] 窗格中，单击 **[Policies （策略）]** 选项卡。随即显示此桌面池的策略页面。

4 在 [Policy Overrides（策略重写）] 框中，单击 **[Add User（添加用户）]**。随即显示 [Policy Override （策略重写）] 窗口。

5 单击 **[Add （添加）]**，为您要向其分配策略的用户输入用户名和描述，然后单击 **[Find Now （立即查找）]**。

> **注释** 如果要查看域中的所有用户列表，请将 **[Name （名称）]** 和 **[Description （描述）]** 字段保留为空。

6 从显示的列表中选择一名或多名用户，并单击 **[OK （确定）]** 返回至 [Policy Override （策略重写）] 窗口。

7 选择您要向其分配新策略的用户，并单击 **[Next （下一步）]**。

8 指定策略设置，并单击 **[OK （确定）]**。现在，已应用用户级别的策略设置。

组策略对象

组策略是 Microsoft Windows NT 系列操作系统的一项功能，它允许您在 Active Directory 环境中对计算机和远程用户进行集中管理和配置。策略属性包含在名为组策略对象 （GPO）的条目中，且可通过 Active Directory 提供的组策略编辑器功能进行配置。

GPO 可应用于整个域内的多个 View Manager 组件，以更精确地控制 View Manager 环境的各个方面。应用后， GPO 属性将存储在指定组件的本地 Windows 注册表中。

为了最大程度地降低创建自定义策略的管理开销，许多组件专用的 GPO 模板已随 View Connection Server 一起提供，您可将其导入至 Active Directory 中。以下是 View Manager 附带的模板文件：

- `vdm_agent.adm`，它包含与 View Agent 控制的客户端桌面身份验证和环境组件相关的属性
- `vdm_client.adm`，它包含与 View Client 的配置参数相关的属性

> **注释** 从 View Connection Server 域外连接的客户端不受 View Client 组件中应用的任何 GPO 的影响。

- `vdm_server.adm`，它包含与 View Connection Server 相关的属性
- `vdm_common.adm`，它包含与 View Manager 所有组件相关的属性

GPO 模板文件存储在以下位置：

```
C:\Program Files\VMware\VMware View\Server\Extras\GroupPolicyFiles
```

Microsoft TechNet 提供了有关如何将 GPO 模板直接加载到 Active Directory 的详细指导：

http://technet.microsoft.com/en-us/library/cc728217.aspx

组策略的应用

GPO 模板加载到 Active Directory 之后，系统将在启动桌面时和用户登录过程中读取并应用这些模板。默认情况下，客户系统大约每隔 90 分钟会对大多数组策略设置进行一次刷新。

注释 组策略更新的时间间隔由常规 Windows 策略控制，也可自行修改。

计算机配置 GPO

使用计算机配置 GPO，无论哪个用户连接到桌面，您都可以设置应用于所有系统的策略。如果用户配置 GPO 中存在等效策略，则该组中包含的策略将会重写。

View Agent 配置

使用表 8-8 和表 8-9 中描述的 GPO 可配置 View Agent 行为。

表 8-8. View Agent 配置属性

属性	描述
`Recursive enumeration of trusted domains`（受信任域的递归枚举）	确定是否枚举代理所在域信任的每个域。为了建立完整的信任链，系统还将枚举每个受信任域所信任的域。该进程将继续递归，直到发现所有受信任的域为止。此信息将传输到 View Connection Server，旨在确保客户端登录后可使用所有受信任的域。 默认情况下，已启用此属性。禁用时，系统仅枚举直接受信任的域，且不会连接到远程域控制器。 **注释：**如果域关系十分复杂（例如，在林中的多个域之间使用多个受信任的林结构），此过程需要数分钟才能完成。

表 8-9. View Agent 配置属性 – 代理配置

属性	描述
`AllowDirectRDP`	确定非 View 客户端是否可以使用 RDP 直接连接到桌面。禁用时，该代理仅允许通过 View Client 或 View Portal 管理 View Manager 连接。 在某个桌面上安装 View Agent 时，若没有同时提供 View Secure Authentication 组件，则此策略对该桌面不会产生影响。 默认情况下，此属性已启用。

表 8-9. View Agent 配置属性 – 代理配置 （续）

属性	描述
AllowSingleSignon	确定是否使用单点登录 （SSO）将用户连接到 View Manager 桌面。已启用时，仅要求用户在连接到 View Client 或 View Portal 时输入凭据。禁用时，用户必须在执行远程连接时重新进行身份验证。 此属性要求在桌面上安装 View Agent 的 Secure Authentication 组件。默认情况下，此属性已启用。
ConnectionTicketTimeout	指定 View 连接票证的有效时间 （以秒为单位）。 连接 View Agent 时， View 客户端使用连接票证进行验证和单点登录。出于安全性原因，连接票证仅在有限时间内有效。当用户连接 View 桌面时，必须在连接票证超时或会话超时之前进行身份验证。 如果未配置此属性，则使用默认超时时限 900 秒。
CredentialFilterExceptions	指定不允许加载代理 CredentialFilter 的可执行文件。文件名不得包含路径或后缀。使用分号分隔多个文件名。
Connect Using DNS Name （使用 DNS 名称连接）	确定 View Connection Server 是否使用计算机的 DNS 名称、而不是其 IP 地址进行连接。在使用 NAT/ 防火墙的情况下，如果 View Client 或 View Connection Server 无法直接使用虚拟桌面的 IP 地址时，则经常使用此属性。 默认情况下，此属性已禁用。
Disable Time Zone Synchronization （禁用时区同步）	确定 View Manager 桌面的时区是否与连接客户端的时区同步。已启用时，仅当 View Client 配置策略的 [Disable time zone forwarding （禁用时区转发）] 属性未设置为 [Disabled （禁用）] 时才可应用此属性。 默认情况下，此属性已禁用。
Toggle Display Settings Control （切换显示设置控制）	确定当客户端会话采用 PCoIP 显示协议时是否禁用 [Display （显示）] 控制面板上的 [Settings （设置）] 选项卡。 默认情况下，此属性已启用。
CommandsToRunOnConnect	列出当客户端登录到某个桌面时将执行的一个或多个命令。有关详细信息，请参阅第 115 页上的 "客户端计算机信息" 。
CommandsToRunOnReconnect	列出当客户端重新连接到含有活动会话的桌面时将执行的一个或多个命令。有关详细信息，请参阅第 115 页上的 "客户端计算机信息" 。

View Client 配置

使用表 8-10、表 8-11 和表 8-12 中描述的 GPO 可配置 View Client 和 View Client with Offline Desktop 行为。

表 8-10. View Client 配置属性

属性	描述
Disable time zone forwarding （禁用时区转发）	确定 View Manager 桌面的时区是否与连接客户端的时区同步。已启用时，仅当 View Agent 配置策略的 [Disable Time Zone Synchronization （禁用时区同步）] 属性未设置为 [Disabled （禁用）] 时才可应用此属性。 默认情况下，此属性已禁用。
Pre-login message precedes smart card PIN request （登录前的消息在智能卡 PIN 请求之前发送）	已启用时，登录前的消息将在智能卡 PIN 请求之前发送。禁用时，登录前的消息将在智能卡 PIN 请求之后发送。 默认情况下，此属性已启用。
Tunnel proxy bypass address list （不使用安全加密链路代理的地址列表）	指定一个安全加密链路地址列表。代理服务器不用于这些地址。使用分号分隔多个条目。
Determines if the VMware View Client should use proxy.pac file（确定 VMware View Client 是否应该使用 proxy.pac 文件）	确定 View Client 是否使用代理自动配置 (Proxy Automatic Configuration, PAC) 文件。如果启用此设置，View Client 就会使用 PAC 文件。 PAC 文件 （通常称为 proxy.pac）可帮助 Web 浏览器和其他用户代理查找适用于特殊 URL 或站点请求的相应代理服务器。 如果在多核计算机上启用此设置，则 View Client 用来查找代理服务器信息的 WinINet 应用程序可能会崩溃。如果您的计算机上出现这种问题，请禁用此设置。 默认情况下，此属性已禁用。
URL for View Client online help（View Client 联机帮助的 URL）	指定一个可供 View Client 检索帮助页面的备用 URL。这项设置适用于因不能访问 Internet 而无法检索远程托管的帮助系统的环境。

表 8-11. View Client 配置属性：脚本定义

属性	描述
Server URL （服务器 URL）	确定 View Client 在登录过程中使用的 URL。例如：http://view1.example.com
Logon UserName （登录用户名）	确定 View Client 在登录过程中使用的用户名。
Logon DomainName （登录域名）	确定 View Client 在登录过程中使用的 NetBIOS 域名。
Logon Password （登录密码）	确定 View Client 在登录过程中使用的密码。 警告：此密码由 Active Directory 存储在纯文本中。

表 8-11. View Client 配置属性：脚本定义 （续）

属性	描述
DesktopName to select （要选择的桌面名称）	确定 View Client 在登录过程中使用的默认桌面。
DesktopLayout (when fully scripted only) （桌面布局 （仅当完全编写了脚本文件时））	指定用户登录 View 桌面时看到的 View Client 窗口布局。 布局选项包括： ■ Full Screen （全屏） ■ Multimonitor （多显示器） ■ Window – Large （窗口 － 大尺寸） ■ Window – Small （窗口 － 小尺寸） 此设置只有在已设置 [DesktopName to select （要选择的桌面名称）] 时才可用。
Suppress error messages (when fully scripted only) （禁止错误消息 （仅当完全编写了脚本文件时））	确定在登录过程中是否显示错误消息。 **注释：**此属性仅适用于已完全编写登录进程脚本文件的情况，即系统已预先通过策略填充所有必要登录信息的情况。 **注释：**如果因输入不正确的登录信息而导致登录失败，则系统不会通知用户，且 View Client wswc.exe 进程将继续在后台运行。

表 8-12. View Client 配置属性 － 安全性设置

属性	描述
Display option to Log in as current user （显示 "作为当前用户登录" 选项））	确定 **[Log in as current user （作为当前用户登录）]** 复选框是否显示在 View Client 连接对话框上。 如果显示该复选框，用户可以选择或取消选择该复选框并重写其默认值。该复选框隐藏时，用户无法重写其默认值。 您可以通过 **[Default value of the 'Log in as current user' checkbox （"作为当前用户登录" 复选框的默认值）]** 策略设置指定 **[Log in as current user （作为当前用户登录）]** 复选框的默认值。 默认情况下，此设置已启用。

表 8-12. View Client 配置属性 – 安全性设置 （续）

属性	描述
Default value of the 'Log in as current user' checkbox（"作为当前用户登录"复选框的默认值）	指定 View Client 连接对话框上 **[Log in as current user （作为当前用户登录）]** 复选框的默认值。 这项设置将重写在 View Client 安装期间指定的默认值。 如果用户通过命令行运行 View Client 并指定了 [logInAsCurrentUser] 选项，则该值将重写此设置。 如果选中了 **[Log in as current user （作为当前用户登录）]** 复选框，用户在登录客户端系统时提供的身份和凭据信息会传送到 View Connection Server 实例，最后传送到 View 桌面。如果取消选择该复选框，用户必须多次输入身份和凭据信息，才能访问 View 桌面。 默认情况下，此设置已禁用。
Brokers Trusted For Delegation（获得委派信任的 Broker）	指定接受用户身份和凭据信息（在用户选中了 **[Log in as current user （作为当前用户登录）]** 复选框时传送）的 View Connection Server 实例。如果您未指定任何 View Connection Server 实例，所有 View Connection Server 实例都会接受该信息。 使用以下某种格式添加 View Connection Server 实例： ■ domain\system$ ■ system$@domain.com ■ View Connection Server 服务的服务主体名称 （Service Principal Name， SPN）。
Ignore incorrect SSL certificate common name (host name field)（忽略不正确的 SSL 证书公用名（主机名字段））	确定是否禁用服务器证书公用名不正确的相关错误。 当证书上的公用名与发送该证书的服务器主机名不相关时，会出现错误。已启用此属性时，系统将忽略此错误。 默认情况下，此属性已禁用。
Ignore bad SSL certificate date received from the server（忽略从服务器中收到的无效 SSL 证书日期）	确定是否禁用服务器证书日期无效的相关错误。 当服务器发送证书的日期已过时，会出现此错误。
Ignore unknown certificate authority problems（忽略未知证书颁发机构问题）	确定是否忽略服务器证书中证书颁发机构未知的相关错误。 当服务器发送的证书是由不受信任的第三方机构签发时，会出现此错误。

表 8-12. View Client 配置属性 – 安全性设置 （续）

属性	描述
Ignore certificate revocation problems（忽略证书吊销问题）	确定是否忽略服务器证书被吊销的相关错误。 当服务器发送的证书被吊销时，会出现此错误。
Ignore incorrect usage problems （忽略用法不正确的问题）	此属性确定是否忽略错误使用服务器证书的相关错误。 当服务器出于其他原因、而不是出于识别发件人并对服务器通信进行加密的目的发送证书时，会出现此错误。
Enable Single Sign-On for smart card authentication（为智能卡身份验证启用单点登录）	确定是否为智能卡身份验证启用单点登录。启用单点登录后， View Client 会将加密的智能卡 PIN 存储到临时内存，然后再将其提交到 View Connection Server。 如果禁用单点登录， View Client 不会显示自定义 PIN 对话框。
Enable jump list integration （启用跳转列表集成）	确定在 Windows 7 及更高版本系统的任务栏上的 View Client 图标中是否显示跳转列表。使用跳转列表，用户可连接最近使用的 View Connection Server 实例和 View 桌面。 共享 View Client 时，您可能不希望用户查看最近使用的桌面名称。因此，您可以通过禁用此设置来禁用跳转列表。 默认情况下，此设置已禁用。

View 公共配置

使用表 8-13 和表 8-14 中描述的 GPO 可配置应用于所有 View Manager 组件的属性：

表 8-13. View Manager 公共配置属性

属性	描述
Enable extended logging（启用扩展日志）	确定跟踪和调试事件是否包含在日志文件中。
Disk threshold for log and events in MegaBytes （日志和事件的磁盘阈值 （以兆字节为单位））	指定日志和事件的最小剩余磁盘空间阈值。如果未指定任何值，则应用默认值 200。达到此值时，将停止记录事件日志。

表 8-14. View Manager 公共配置 – 日志配置

属性	描述
Number of days to keep logs（保留日志的天数）	指定日志文件在系统中保留的天数。如果未设置任何值，则应用默认值，日志文件仅保留 7 天。

View Server 配置

使用表 8-15 中介绍的 GPO 可配置应用于 View Connection Server 的设置：

表 8-15. View Manager Server 配置属性

属性	描述
Recursive enumeration of trusted domains （受信任域的递归枚举）	确定是否枚举服务器所在域所信任的每个域。为了建立完整的信任链，系统还将枚举每个受信任域所信任的域。该进程将继续递归，直到发现所有受信任的域为止。此信息将传输到 View Connection Server，旨在确保客户端登录后可使用所有受信任的域。 默认情况下，已启用此属性。禁用时，系统仅枚举直接受信任的域，且不会连接到远程域控制器。 **注释：**如果域关系十分复杂 （例如，在林中的多个域之间使用多个受信任的林结构），此过程需要数分钟才能完成。

用户配置 GPO

使用用户配置 GPO，无论用户连接到哪个桌面，您都可以设置应用于用户的策略。这些策略可重写已应用于目标桌面的任何等效的计算机配置策略。

View Agent 配置

使用表 8-16 中描述的 GPO 可配置 View Agent 行为。

表 8-16. View Agent 配置属性 – 代理配置

属性	描述
Disable Time Zone Synchronization （禁用时区同步）	确定 View 桌面的时区是否与 View 客户端的时区同步。 已启用时，仅当 View Client 配置策略的 [Disable time zone forwarding （禁用时区转发）] 属性已禁用时，才可应用此属性。 默认情况下，此属性已禁用。

View Client 配置

使用表 8-17、表 8-18、表 8-19 和表 8-20 中描述的 GPO 可配置 View Client 和 View Client with Offline Desktop 行为。

表 8-17. View Client 配置属性

属性	描述
Disable time zone forwarding （禁用时区转发）	确定 View 桌面的时区是否与连接客户端的时区同步。已启用时，仅当 View Agent 配置策略的 [Disable Time Zone Synchronization （禁用时区同步）] 属性已禁用时，才可仅应用此属性。 默认情况下，此属性已禁用。
Enable the shade （启用幕帘）	确定是否启用 [View Client] 窗口顶部的幕帘 [菜单栏]。 默认情况下，此属性已启用。
Pin the Shade （固定幕帘）	确定是否启用在 [View Client] 窗口顶部的幕帘中的大头针，以阻止自动隐藏菜单栏。 **注释：**禁用幕帘时，此属性无效。 默认情况下，此属性已启用。
Always on top （总在最前面）	确定 View Client 窗口是否总显示在最前面。启用此设置可避免 Windows 任务栏遮挡全屏模式的 View Client 窗口。默认情况下，此设置已启用。
Don't check monitor alignment on spanning （横跨时不检查监视器是否对齐）	默认情况下，如果屏幕组合在一起时未形成精确矩形（即监视器位于左侧及右侧时，屏幕高度相同；监视器位于顶部及底部时，屏幕宽度相同），客户端桌面不会横跨多个监视器。 此属性可重写此规则。默认情况下，此属性已禁用。
Enable multi-media acceleration （启用多媒体加速）	指定是否在客户端中启用多媒体重定向 （MMR）。MMR 是指一种直接通过 TCP 套接字将多媒体数据从远程桌面中的特定编解码器转发至客户端的 Microsoft DirectShow Filter。转发后，数据直接在播放数据的客户端中进行解码。 如果客户端资源不足，无法处理本地多媒体解码，则管理员可禁用 MMR。 **注释：**如果 View Client 视频显示硬件不支持覆盖功能，MMR 将无法正常运行。 MMR 策略不适用于 Offline Desktop 会话。

表 8-18. View Client 配置属性 － 脚本定义

属性	描述
Server URL （服务器 URL）	确定 View Client 在登录过程中使用的 URL。例如：`http://view1.example.com`
Logon UserName （登录用户名）	确定 View Client 在登录过程中使用的用户名。
Logon DomainName （登录域名）	确定 View Client 在登录过程中使用的 NetBIOS 域名。
Logon Password （登录密码）	确定 View Client 在登录过程中使用的密码。 **警告：**此密码由 Active Directory 存储在纯文本中。
DesktopName to select （要选择的桌面名称）	确定 View Client 在登录过程中使用的默认桌面。
DesktopLayout (when fully scripted only) （桌面布局 （仅当完全编写了脚本文件时））	指定用户登录 View 桌面时看到的 View Client 窗口布局。 布局选项包括： ■ Full Screen （全屏） ■ Multimonitor （多显示器） ■ Window - Large （窗口 － 大尺寸） ■ Window - Small （窗口 － 小尺寸） 此设置只有在已设置 [DesktopName to select （要选择的桌面名称）] 时才可用。
Suppress error messages (when fully scripted only) （禁止错误消息 （仅当完全编写了脚本文件时））	确定在登录过程中是否显示错误消息。 如果因输入不正确的登录信息而导致登录失败，则系统不会通知用户，且 View Client `wswc.exe` 进程将继续在后台运行。
Disable 3rd-party Terminal Services plugins （禁用第三方终端服务插件）	将该属性设置为 True 后，将不会检查有无第三方终端服务插件已安装为一般 RDP 插件。此设置不会影响 View 特定插件，如 USB 重定向。如果未配置此策略，则默认情况下就会检测并使用第三方插件。

表 8-19. View Client 配置属性 – RDP 设置

属性	描述
Color Depth （颜色深度）	确定远程桌面的颜色深度。 已启用此属性时，可用的设置包括： ■ 8 ■ 15 ■ 16 ■ 24 ■ 32 **注释：**对于 24 位 Windows XP 系统，确保将以下 [Computer Configuration GPO（计算机配置 GPO 属性）] 设置为 [Enabled （启用）] 和 [24 bit （24 位）]： [Computer Configuration （计算机配置）] > [Administrative Templates （管理模板）] > [Windows Components （Windows 组件）] > [Terminal Services（终端服务）] > [Limit Maximum Color Depth （限制最大颜色深度）]
Desktop Background （桌面背景）	确定客户端连接到远程桌面时是否显示桌面背景。
Show contents of window while dragging （拖动时显示窗口内容）	确定用户将文件夹拖到新位置时是否显示文件夹内容。
Menu and window animation （菜单和窗口动画）	确定客户端连接到远程计算机时菜单和窗口的行为方式。
Themes （主题）	确定客户端连接到远程桌面时是否显示主题。
Cursor shadow （光标卷影）	确定是否在远程桌面的光标下方显示卷影。
Font smoothing （字体平滑）	（适用于 Windows Vista 或更高版本）确定是否对远程桌面的字体应用消除锯齿。
Desktop composition （桌面拼合）	（适用于 Windows Vista 或更高版本）确定是否在远程桌面中启用桌面拼合。 启用桌面拼合时，单个窗口不再像在先前的 Microsoft Windows 版本中那样可直接绘制到屏幕或主要显示设备中。相反，其图形将重定向到视频内存的屏幕外表上，然后呈现为桌面映像，并在显示器中显示。

表 8-19. View Client 配置属性 – RDP 设置 （续）

属性	描述
Audio redirection （音频重定向）	确定在远程桌面中播放时音频信息的播放方式。 已启用此属性时，可用的设置包括： ■ [Disable Audio （禁用音频）]：无音频 ■ [Play in VM (needed for VoIP USB support)（在虚拟机中播放 （VoIP USB 支持的必备条件）]：音频在远程桌面内播放 （需要共享 USB 音频设备才能在客户端中播放声音） ■ [Redirect to client （重定向到客户端）]：音频重定向到客户端。这是默认模式。 此属性仅适用于 RDP 音频，客户端中将播放通过 MMR 重定向的音频。
Redirect drives （重定向驱动器）	确定客户端连接到远程计算机时是否自动重定向本地磁盘驱动器。
Redirect printers （重定向打印机）	确定客户端连接到远程桌面时是否自动重定向本地打印机。
Redirect serial ports （重定向串行端口）	确定客户端连接到远程桌面时是否自动重定向本地 COM 端口。
Redirect smart cards （重定向智能卡）	确定客户端连接到远程桌面时是否自动重定向本地智能卡。
Redirect clipboard （重定向剪贴板）	此设置确定客户端连接到远程桌面时是否自动重定向本地剪贴板信息。
Redirect supported plug and play devices （重定向受支持的即插即用设备）	确定客户端连接到远程桌面时是否自动重定向本地即插即用的设备和 POS 终端设备。这与 View Agent 的 USB 重定向组件管理的重定向不同。
Bitmap caching （位图缓存）	确定远程位图是否缓存在本地计算机中。
Shadow bitmaps （卷影位图）	确定是否应使用卷影位图。 全屏模式中始终禁用卷影位图，因此，处于全屏模式时，此属性无效。
Cache persistence active （缓存永久活动）	确定是否应使用永久位图缓存。永久缓存可提高性能，但需要更多磁盘空间。
Enable compression （启用压缩）	确定是否使用 RDP 数据压缩。默认情况下，已启用压缩。
Windows key combination redirection （Windows 按键组合重定向）	确定应用 Windows 按键组合的位置。 已启用此属性时，可用的设置包括： ■ Apply key combinations locally （本地应用按键组合） ■ Send key combinations to VM （将按键组合发送至虚拟机）

表 8-19. View Client 配置属性 – RDP 设置 （续）

属性	描述
Enable Credential Security Service （启用凭据安全服务）	指定 View 桌面连接是否使用网络级别身份验证（Network Level Authentication， NLA）。在 Windows Vista 中，远程桌面连接默认情况下需要使用 NLA。 如果客户操作系统需要使用 NLA 进行远程桌面连接，您必须启用该设置，否则 View Client 将无法连接到 View 桌面。 除了启用该设置，您还必须满足以下条件： ■ 客户端和客户操作系统都要支持 NLA。 ■ 启用 View Connection Server 实例的客户端直接连接。使用 NLA 时，不支持安全加密链路连接。 ■ View Secure Authentication 组件未安装在客户操作系统的 View Agent 中。使用 NLA 时，不支持单点登录。
Bitmap cache file size in Kb for 8bpp bitmaps （适用于 8bpp 位图的缓存文件大小（以 KB 为单位））	指定用于 8 位 / 像素增强色设置的永久位图缓存文件大小（以 KB 为单位）。 启用此属性时，需要输入文件大小 （以 KB 为单位）。
Bitmap cache file size in Mb for 8bpp bitmaps （适用于 8bpp 位图的缓存文件大小（以 MB 为单位））	指定用于 8 位 / 像素增强色设置的永久位图缓存文件大小（以 MB 为单位）。 启用此属性时，需要输入文件大小 （以 MB 为单位）。
Bitmap cache file size in Mb for 16bpp bitmaps （适用于 16bpp 位图的缓存文件大小（以 MB 为单位））	指定用于 16 位 / 像素增强色设置的永久位图缓存文件大小（以 MB 为单位）。 启用此属性时，需要输入文件大小 （以 MB 为单位）。
Bitmap cache file size in Mb for 24bpp bitmaps （适用于 24bpp 位图的缓存文件大小（以 MB 为单位））	指定用于 24 位 / 像素增强色设置的永久位图缓存文件大小（以 MB 为单位）。 启用此属性时，需要输入文件大小 （以 MB 为单位）。
Bitmap cache file size in Mb for 32bpp bitmaps （适用于 32bpp 位图的缓存文件大小（以 MB 为单位））	指定用于 32 位 / 像素增强色设置的永久位图缓存文件大小（以 MB 为单位）。 启用此属性时，需要输入文件大小 （以 MB 为单位）。

表 8-20. View Client 配置属性 – 安全性设置

属性	描述
Display option to Log in as current user （显示 "作为当前用户登录" 选项）)	确定 **[Log in as current user （作为当前用户登录）]** 复选框是否显示在 View Client 连接对话框上。 如果显示该复选框，用户可以选择或取消选择该复选框并重写其默认值。该复选框隐藏时，用户无法重写其默认值。 您可以通过 **[Default value of the 'Log in as current user' checkbox （"作为当前用户登录" 复选框的默认值）]** 策略设置指定 **[Log in as current user（作为当前用户登录）]** 复选框的默认值。 默认情况下，此设置已启用。
Default value of the 'Log in as current user' checkbox （"作为当前用户登录" 复选框的默认值）	指定 View Client 连接对话框上 **[Log in as current user （作为当前用户登录）]** 复选框的默认值。 当选择了该复选框时，用户在登录客户系统时提供的身份和凭据信息会传送到 View Connection Server 实例，最后传送到 View 桌面。如果取消选择该复选框，用户必须多次输入身份和凭据信息，才能访问 View 桌面。 该设置指定的默认值在以下情况下会被重写： ■ 如果用户曾通过命令行运行 View Client，并为该复选框指定了其他值，则新值将替换默认值。 ■ 如果用户之前运行过 View Client，并为 View Client 连接对话框上的复选框选择了其他值，则新值将替换默认值。 在命令行中指定的复选框值优先于 View Client 连接对话框中指定的值。 默认情况下，此设置已禁用。

统一访问 9

大型企业经常混合使用物理 PC 机、基于服务器的桌面或通过终端服务、虚拟桌面和刀片 PC 发布的应用程序。需要访问多个平台的用户必须使用多个不同的界面。统一访问支持 View Manager 提供统一界面，通过此界面，用户可访问由多个后端计算机交付的桌面。

本章中使用的 “桌面源” 术语是指终端服务器、物理计算机或未被管理的虚拟机。

本章讲述以下主题：

准备各种可被远程访问的后端计算机

必须准备桌面源才可交付桌面访问。如果桌面源不满足以下条件，则远程桌面交付将失败。

- 在后端计算机中安装 View Agent。有关安装 View Agent 的更多信息，请参阅第 194 页上的 “在未被管理的桌面源中安装 View Agent”。
- 确保后端计算机满足以下要求：
  - 后端计算机与 View 服务器位于相同域中，或位于受信任的域中，以启用单点登录。
  - 允许所需的域用户或用户组远程连接到计算机，以启用单点登录。
- 确保未被 vCenter Server 管理的后端计算机已启动，并确保 View Connection Server 可以访问该计算机。
- 在后端计算机中启用 RDP 连接。

满足以上条件时，后端计算机便可用来交付远程桌面。

桌面参数

当您正在配置被管理和未被管理的单个桌面、桌面池和终端服务器时，必须设置桌面参数。对于被管理和未被管理的资源，桌面参数有所不同。本部分将阐述桌面参数的重要性，并介绍桌面资源及其特定参数之间的映射方式。

表 9-1 介绍了所有桌面参数。

表 9-1. 桌面参数

属性	参数描述
Desktop pool state （桌面池状态）	**Enabled （启用）** – 创建桌面池后，自动启用桌面池并准备立即投入使用。 **Disabled （禁用）** – 创建桌面池后，将禁用桌面池，桌面池不可使用。如果要执行部署后的活动，如测试或其他形式的基准维护，则该设置很适用。
Virtual machine power policy （虚拟机电源策略）	**Do nothing （VM remains on）（不执行任何操作 （虚拟机始终打开））** – 您可根据需要启动已关闭的虚拟机并保持打开状态，即使在不使用时仍亦如此，直到关机为止。 **Ensure VM is always powered on （确保始终启动虚拟机）** – 池中所有虚拟机始终均启动，即使在不使用时仍亦如此。如果虚拟机已关机，则系统将立即重新启动虚拟机。 **Suspend （挂起）** – 不使用时，池中所有虚拟机都将进入挂起状态。 **Power off （关闭）** – 不使用时，池中所有虚拟机都将关机。

表 9-1. 桌面参数 （续）

属性	参数描述
Automatic logoff after disconnect （断开连接后自动注销）	**Immediately** （立即） － 用户在断开连接后立即注销。 **Never** （从不） － 用户从不注销。 **After** （之后） － 指用户断开连接后，在此时间过后即注销用户。输入持续时间 （以分钟为单位）。
Power off and delete virtual machine after first use （首次使用后关闭并删除虚拟机）	用户注销后立即删除虚拟机。 如有必要，在删除虚拟机后，可以克隆新虚拟机以维护特定池的大小。
Allow users to reset their desktop （允许用户重置桌面）	允许用户在没有管理协助的情况下重置其桌面。
Allow multiple sessions per user （允许每个用户多个会话）	允许单个用户同时连接到同一池中的多个桌面。

表 9-2 列出了每种桌面类型适用的参数。

表 9-2. 桌面参数到桌面类型的映射一览表

参数	单个被管理的桌面	单个未被管理的桌面	手动管理池		手动的未被管理池		终端服务器池
			永久	非永久	永久	非永久	
Desktop state （桌面状态）	是	是	是	是	是	是	是
Virtual machine power policy （虚拟机电源策略）	是		是	是			
Automatic logoff after disconnect （断开连接后自动注销）	是	是	是	是	是	是	是
Allow users to reset their desktop （允许用户重置桌面）	是		是	是			
Allow multiple sessions per user （允许每个用户多个会话）				是		是	

在未被管理的桌面源中安装 View Agent

在安装过程中，安装程序将检测何时在未被管理的桌面源中安装该代理。未被管理的桌面源是指未在 ESX 主机中运行的虚拟机。与此同时，还可使用 View Connection Server 注册桌面源。注册后，指定的 View Connection Server 及其副本实例可以与该桌面源进行通信。

此部分介绍如何在未被管理的桌面源中安装 View Agent。有关在被管理的桌面源中安装 View Agent 的信息，请参阅第 66 页上的 "准备客户系统"。

在未被管理的桌面源中安装 VMware View Agent

1 在要安装该代理的系统中运行 View Agent 可执行文件，其中 xxx 指文件的内部版本号：

   ```
   VMware-viewagent-e.x.p-xxx.exe
   ```

   将打开安装向导。单击 **[Next （下一步）]**。

2 接受 VMware 许可条款并单击 **[Next （下一步）]**。

3 选择自定义的安装选项。

   接受或更改目标文件夹，并单击 **[Next （下一步）]**。

4 在 **[Register with View Connection Server （使用 View Connection Server 注册）]** 窗口中，指定服务器名或 IP 地址。

   IP 地址可以是 View Connection Server 的标准实例或副本实例。

5 提供管理员登录凭据，以便使用 View Connection Server 注册此计算机，然后单击 **[Next （下一步）]**。

   您可以以当前用户的身份登录。如果选择此选项，请禁用 **[Username （用户名）]** 和 **[Password （密码）]** 字段。

   您可指定管理员凭据。指定 View Connection Server 管理员的用户名和密码。

6 将显示安装选项。

   单击 **[Next （下一步）]** 以确认并继续进行安装。

7 请单击 **[Install （安装）]** 开始安装。

   完成安装后，单击 **[Finish （完成）]**。

现在，未被管理的桌面源已做好准备，可随时使用。

添加和更改桌面源

在桌面源中执行端到端配置，确保轻松解决安装和配置问题。此部分涵盖单个桌面或桌面池。

添加未被管理的单个桌面

1 确保您已拥有适当的登录凭据，并登录到 View Administrator。

2 在 **[Desktops （桌面）]** 选项卡中，单击 **[Add （添加）]**

3 在 **[Desktop Type （桌面类型）]** 窗口中，选择 **[Individual Desktop （单个桌面）]**，并单击 **[Next （下一步）]**。

4 在 **[Desktop Source （桌面源）]** 窗口中，选择 **[Physical computers or virtual machines not managed by a vCenter Server（未被 vCenter Server 管理的物理机或虚拟机）]**，并单击 **[Next （下一步）]**。

5 输入 **[Unique ID （唯一 ID）]**、 **[Display name （显示名称）]** 和 **[Description （描述）]**。

[Unique ID（唯一 ID）] 是指 View Manager 用来识别桌面的名称。桌面 [Display name （显示名称）] 是用户登录时看到的名称。您可随意输入 [Unique ID （唯一 ID）] 和 [Display name （显示名称）]，但如果您未指定 [Display name （显示名称）]，则系统会将 [Unique ID （唯一 ID）] 同时用作 [Display name （显示名称）]。如果有多个 VirtualCenter 或 vCenter Server，请参见第 201 页上的 "唯一 ID 的唯一性"。

注释 对于可选描述，您可以使用包括空格在内的任何字母数字字符。[Description （描述）] 最多为 1024 个字符，且仅可从 [View Administrator] 界面内查看。

提供桌面标识的详细信息后，请单击 **[Next （下一步）]**。

6 指定桌面参数，并单击 **[Next （下一步）]**。

有关适用于未被管理的单个桌面的参数的更多信息，请参阅第 193 页上的表 9-2， "桌面参数到桌面类型的映射一览表"。

7 在 **[Desktop Source （桌面源）]** 页面的表中，选择要添加为单个桌面的桌面源，并单击 **[Next （下一步）]**。

您仅可选择一个桌面源。该表将显示所有正在运行支持客户端操作系统的已注册桌面源、以及尚未投入使用的其他桌面或桌面池。有关注册桌面源的更多信息，请参阅第 194 页上的 "在未被管理的桌面源中安装 View Agent"。

8 浏览 **[Ready to Complete （准备完成）]** 中的信息，并单击 **[Finish （完成）]** 接受默认值，或 **[Back （返回）]** 以进行更改。

9 单击 **[Finish （完成）]**。

桌面已添加，并显示在 **[Desktops （桌面）]** 主页中。

添加未被管理的手动池

1 确保您已拥有适当的登录凭据，并登录到 View Administrator。

2 在 **[Desktops （桌面）]** 选项卡中，单击 **[Add （添加）]**。

3 在 **[Desktop Type （桌面类型）]** 窗口中，选择 **[Manual Desktop Pool （手动桌面池）]**，并单击 **[Next （下一步）]**。

4 在 **[Desktop Persistence （桌面永久性）]** 窗口中，为该池中的桌面指定永久设置。

Persistent （永久） – 此桌面池允许用户每次登录到相同桌面。由于用户总是返回到相同桌面，因此，他们可以将文档和文件保存在永久桌面中。

Non-persistent （非永久） – 指允许用户登录、但用户注销时将返回到池的桌面。用户每次登录到不同桌面，且无法将文档或文件保存在桌面中。

5 在 **[Desktop Pool Source （桌面池源）]** 窗口中，选择 **[Physical computers or virtual machines not managed by a vCenter Server （未被 vCenter Server 管理的物理机或虚拟机）]**，并单击 **[Next （下一步）]**。

6 输入 **[Unique ID （唯一 ID）]**、 **[Display name （显示名称）]** 和 **[Description （描述）]**。

[Unique ID（唯一 ID）] 是指 View Manager 用来识别桌面的名称。桌面 [Display name （显示名称）] 是用户登录时看到的名称。您可随意输入 [Unique ID （唯一 ID）] 和 [Display name （显示名称）]，但如果您未指定 [Display name （显示名称）]，则系统会将 [Unique ID （唯一 ID）] 同时用作 [Display name （显示名称）]。如果有多个 VirtualCenter 或 vCenter Server，请参见第 201 页上的 "唯一 ID 的唯一性"。

注释 对于可选描述，您可以使用包括空格在内的任何字母数字字符。[Description （说明）] 最多为 1024 个字符，且仅可从 View Administrator 界面内查看。

提供桌面标识的详细信息后，请单击 **[Next （下一步）]**。

7 指定桌面参数，并单击 **[Next （下一步）]**。

有关适用于未被管理的永久或非永久池的参数的更多信息，请参阅第 193 页上的表 9-2， "桌面参数到桌面类型的映射一览表"。

8 在 **[Desktop Source （桌面源）]** 页面的表中，选择池中要包含的桌面源，并单击 **[Next （下一步）]**。

   该表将显示所有正在运行支持客户端操作系统的已注册桌面源、以及尚未投入使用的其他桌面或桌面池。有关注册桌面源的更多信息，请参阅第 194 页上的 “在未被管理的桌面源中安装 View Agent”。

9 浏览 **[Ready to Complete （准备完成）]** 中的信息，并单击 **[Finish （完成）]** 接受默认值，或 **[Back （返回）]** 以进行更改。

10 单击 **[Finish （完成）]**。

   桌面已成功添加，并显示在 **[Desktops （桌面）]** 主页中。

添加终端服务器池

1 确保您已拥有适当的登录凭据，并登录到 View Administrator。

2 在 **[Desktops （桌面）]** 选项卡中，单击 **[Add （添加）]**。

3 在 **[Desktop Type （桌面类型）]** 窗口中，选择 **[Microsoft Terminal Services Desktop Pool （Microsoft Terminal Services 桌面池）]**，并单击 **[Next （下一步）]**。

4 输入 **[Unique ID （唯一 ID）]**、 **[Display name （显示名称）]** 和 **[Description （描述）]**。

   [Unique ID（唯一 ID）] 是指 View Manager 用来识别桌面的名称。桌面 [Display name （显示名称）] 是用户登录时看到的名称。您可随意输入 [Unique ID （唯一 ID）] 和 [Display name （显示名称）]，但如果您未指定 [Display name （显示名称）]，则系统会将 [Unique ID （唯一 ID）] 同时用作 [Display name （显示名称）]。如果有多个 VirtualCenter 或 vCenter Server，请参见第 201 页上的 “唯一 ID 的唯一性”。

   注释 对于可选描述，您可以使用包括空格在内的任何字母数字字符。[Description （描述）] 最多为 1024 个字符，且仅可从 [View Administrator] 界面内查看。

   提供桌面标识的详细信息后，请单击 **[Next （下一步）]**。

5 指定桌面参数，并单击 **[Next （下一步）]**。

   有关适用于终端服务器池的参数的更多信息，请参阅第 193 页上的表 9-2， “桌面参数到桌面类型的映射一览表”。

6 单击 **[Next （下一步）]**。

7 在 **[Desktop Source （桌面源）]** 页面的表中，选择桌面池中要包含的终端服务源，并单击 **[Next （下一步）]**。

该表将显示所有正在运行支持客户端操作系统的已注册桌面源、以及尚未投入使用的其他终端服务器池。有关注册桌面源的更多信息，请参阅第 194 页上的 "在未被管理的桌面源中安装 View Agent"。

8 浏览 **[Ready to Complete （准备完成）]** 中的信息，并单击 **[Finish （完成）]** 接受默认值，或 **[Back （返回）]** 以进行更改。

9 单击 **[Finish （完成）]**。

桌面已添加，并显示在 **[Desktops （桌面）]** 主页中。

启用或禁用桌面

您仅可访问已启用的桌面。

启用或禁用桌面

1 在 [Desktops （桌面）] 选项卡中，选择一个桌面并单击 **[Enable/Disable （启用 / 禁用）]**。

如果该桌面当前已启用，则可以禁用它；如果该桌面当前已禁用，则可以启用它。

2 选择 **[Enable Desktop （启用桌面）]** 或 **[Disable Desktop （禁用桌面）]** （如适用），并单击 **[OK （确定）]**。

将用户和用户组授权给桌面

添加桌面或桌面池后，您必须对其授权，以便用户和用户组可以访问这些桌面或桌面池。一个桌面可以分配给多个用户或多个用户组。

授权用户和用户组

1 在 **[Desktops （桌面）]** 选项卡中，选择一个桌面或桌面池，并单击 **[Entitle （授权）]**。

2 在 **[Entitlement （授权）]** 窗口中，单击 **[Add （添加）]** 以添加用户或用户组。

3 指定搜索标准，以检索用户或用户组列表，并单击 **[Find Now （立即查找）]**。

将显示用户和 / 或用户组列表。

4 选择要授权使用此桌面源的用户或用户组，并单击 **[OK （确定）]**。

该用户或用户组将在 **[Entitlement （授权）]** 窗口中显示。

5 选择该用户或用户组，并单击 **[Remove （删除）]** 以阻止其访问桌面。

6 单击 **[OK （确定）]** 以返回到 **[Desktops （桌面）]** 选项卡。

添加或删除桌面源

您可从桌面池中添加或删除桌面源。

将桌面源添加到桌面池

1 在 [Desktop （桌面）] 窗格中，选择一个桌面池并单击 **[Desktop Sources （桌面源）]** 选项卡。

2 单击 **[Add （添加）]** 将桌面源添加到池中。

3 选择该池中要包含的桌面源，并单击 **[OK （确定）]**。

   您将返回主页，该页面将列出该池中的所有桌面源。

从桌面池中删除桌面源

1 在 [Desktop （桌面）] 窗格中，选择一个桌面池并单击 **[Desktop Sources （桌面源）]** 选项卡。

2 选择桌面源，并单击 **[Remove （删除）]**。

   将显示配置消息。

3 单击 **[OK （确定）]**，将从该池中删除选定桌面源。

4 如果其中任何一个桌面源包含活动会话，请指定要执行的操作：

   - **Leave active （保留活动）**：活动会话将保留，直到用户注销为止。 View Connection Server 不会跟踪这些会话。
   - **Terminate （终止）**：立即终止所有活动会话。

5 您将返回主页，该页面不再列出已删除的桌面源。

更改单个桌面源

如果只有一个桌面，则无法添加或删除桌面源。但您可以更改或重置桌面源。此部分仅适用于单个桌面，而不适用于桌面池。

更改单个桌面源

1 在 [Desktop （桌面）] 窗格中，选择单个桌面并单击 **[Desktop Sources （桌面源）]** 选项卡。

2 选择该桌面源，并单击 **[Change （更改）]**。

3 选择桌面要使用的虚拟机，并单击 **[OK （确定）]**。

   该表将显示所有正在运行支持客户端操作系统的可用虚拟机、以及尚未投入使用的其他虚拟机，其中包括挂起或未启动的虚拟机。

   将显示确认页面。

4 单击 **[OK （确定）]** 将原始桌面源更改为选定的桌面源。

5 您将返回到主页，主页中将显示已更改的桌面源。

删除桌面

您可以删除单个桌面或桌面池。

要删除未被管理的桌面，则必须取消注册这些桌面。请参阅 "取消注册桌面源。"

删除未被管理的桌面池

1 在 **[Desktops （桌面）]** 选项卡中，选择未被管理的桌面池或桌面，并单击 **[Delete （删除）]**。

   将显示一条警告消息，指出您试图永久性删除此桌面池。

   系统仅删除该桌面池，而不会删除属于该池的未被管理桌面的注册信息。

2 如果其中任何一个桌面源包含活动会话，请选择要执行的操作：

   - **Leave active （保留活动）**： 活动会话将保留，直到用户注销为止。 View Connection Server 不会跟踪这些连接。
   - **Terminate （终止）**： 立即终止所有活动会话。

3 单击 **[OK （确定）]** 以删除桌面池，并返回到主页。

取消注册桌面源

安装 View Agent 时，系统将注册 vCenter Server 管理的所有桌面源。有关安装 View Agent 的更多信息，请参阅第 194 页上的 "在未被管理的桌面源中安装 View Agent"。您仅可取消注册未被管理的桌面源。

取消注册未被管理的桌面源

1 单击 **[Configuration （配置）]** 选项卡。

   [Registered Desktop Sources （已注册的桌面源）] 部分将显示已注册的终端源和其他未被管理的虚拟机。

2 选择桌面源类型，并单击 **[View （查看）]**。

3 选择要取消注册的桌面源，并单击 **[Unregister （取消注册）]**。

   您仅可选择尚未分配给桌面的桌面源。

   将显示一条消息，检查您是否要取消注册桌面源。如果取消注册桌面源，则该桌面源将不可用。要使这些桌面源重新可用，请在每个桌面源中重新安装 View Agent。

4 如果要取消注册选定的桌面源，请单击 **[OK （确定）]**。

桌面源已取消注册，并不再可用。

唯一 ID 的唯一性

如果当前环境中运行了多个 VirtualCenter 或 vCenter Server，请确保其他 VirtualCenter 或 vCenter Server 没有使用相同的唯一 ID。默认情况下，唯一 ID 是随机生成的，但您也可以对它进行编辑。关于编辑唯一 ID 值的详细信息，请参见 VMware Infrastructure 或 vSphere 文档。

故障排除 10

管理员或用户在使用 View Manager 产品时，可能会遇到异常情况。如果出现异常情况，您可从 VMware 处获得帮助。

本章概述了某些高级步骤，帮助您收集应用程序数据、请求帮助，以及在知识库中搜索支持信息。

本章将讲述以下主题：

收集 View Manager 的诊断信息

诊断信息有助于 VMware 技术支持部门诊断并解决问题。View Manager 附带了一个名为 `vdm-support` 的脚本，该脚本将收集 VMware 技术支持部门要使用的信息。请将该脚本生成的文件与您的支持请求一起发送。

在 View Connection Server 中，您可以手动运行该脚本，或通过使用 **[Start （开始）]** 菜单中的支持工具运行。对于 View Client 或正在运行 View Agent 的 View Manager 桌面，您必须手动运行该脚本。

使用 View Manager 支持工具收集诊断信息

使用 View Manager 支持工具，您可以生成日志文件，并设置日志级别，确定需要为 View Connection Server 生成常规日志文件、调试日志文件，还是完整日志文件。

使用 View Manager 支持工具设置日志级别

1 在 View Connection Server 中，依次单击 **[Start（开始）]**、**[All Programs （所有程序）]** 和 **[VMware]**。

2 选择 **[Set View Connection Server Log Levels（设置 View Connection Server 日志级别）]**。

3 在 **[Choice （选项）]** 字段中，针对常规、调试和完整日志文件分别键入 `1`、`2`、`3`，或键入 `0` 将日志设置重置为默认值。然后按 **Enter** 键。

默认的日志级别为调试级别。

使用 View Manager 支持工具生成日志文件

1 在 View Connection Server 中，依次单击 **[Start（开始）]**、**[All Programs （所有程序）]** 和 **[VMware]**。

2 选择 **[Generate View Connection Server Log Bundle （生成 View Connection Server 日志捆绑包）]**。

该支持工具将创建一个名为 `vdm-sdct`、且包含已生成日志文件的文件夹，并将它放在 View Connection Server 的桌面中。

使用 View Manager 支持脚本收集诊断信息

使用 View Manager 支持脚本为 View Connection Server、 View Client、 View Portal 以及运行 View Agent 的 View Manager 桌面生成日志文件。

使用脚本收集诊断信息

1 打开命令提示符，并转到 View Manager 程序目录。每个 View Manager 组件的位置如下所示：

- View Connection Server -
  `C:\Program Files\VMware\VMware View\Server\DCT`
- View Client 或 View Portal -
  `C:\Program Files\VMware\VMware View\Client\DCT`
- 运行 View Agent 的 View Manager 桌面 -
  `C:\Program Files\VMware\VMware View\Agent\DCT`

注释 如果未将程序安装在默认目录中，请替换相应的驱动器号和路径。

---

2 运行以下支持脚本：

```
cscript vdm-support.vbs
```

运行脚本后，系统将向您显示输出文件名和位置。

3 在 VMware 网站的支持页面中提交支持请求。

View Composer 支持

通过收集配置数据和登录数据， View Manager 附带的 `svi-support` 脚本可为 View Composer 提供针对特定组件的支持。收集此信息，旨在帮助 VMware 客户支持部门诊断当使用此功能时可能出现的任何问题。

必须使用 Windows Script Host（提供用来设置脚本属性的命令行选项）的命令行版本 `cscript.exe` 来运行 svi-support 脚本。 Microsoft TechNet 提供了有关如何使用 `cscript.exe` 的详细指导，网址为：

http://technet.microsoft.com/library/bb490887.aspx

`svi-support` 脚本位于 vCenter Server 中，与 View Composer 服务软件位于同一目录下：

```
C:\Program Files\VMware\VMware View Composer
```

使用 Windows 命令提示符提交 `svi-support` 脚本说明时，需要采用以下格式：

```
cscript.wsf svi-support.wsf [/?] [/novclogs] [/dmpdir:< 值 >]
[/dmpformat:< 值 >] [/nolog] [/fullbundle] [/filescount:< 值 >]
[/destdir:< 值 >] [/logdir:< 值 >] [/logformat:< 值 >] [/zip:< 值 >]
```

与该工具关联的所有参数均为可选参数，前面必须带有正斜线 （/）。表 10-1 中详细描述了这些参数。

表 10-1. svi-support — 参数

参数	描述
?	显示与支持脚本结合使用的参数。
novclogs	vCenter Server 含有诊断脚本，这些脚本可从 vCenter Server 应用程序日志中收集服务器和数据库相关信息。如果要禁用从 vCenter Server 日志中收集信息，请指定此选项。
dmpdir	从中收集 View Composer 日志的目录的绝对路径。 默认路径为： `%ALLUSERSPROFILE%\Application Data\VMware\View Composer\Logs`

表 10-1. svi-support － 参数 （续）

参数	描述
dmpformat	用来过滤 dmp 文件的前缀。 默认值为 vmware-svi-
nolog	禁用系统事件日志记录事件。
fullbundle	生成包含扩展数据在内的完整捆绑包。此步骤最多需要 10 分钟的时间；默认情况下省略该步骤。
filescount	从每个文件夹位置收集的最大文件数。默认值为 50。
destdir	用来保存日志数据的目录的绝对路径。默认目录为当前用户的 Windows 桌面目录。如果已指定目录，请确保目录权限可保证日志数据的安全。
logdir	从中收集日志的目录路径。默认路径为： %ALLUSERSPROFILE%\Application Data\VMware\View Composer\Logs
logformat	用来过滤日志文件的前缀。默认值为 vmware-desktopcomposer
zip	指定用来将支持信息存档的实用程序。如果未指定任何值，则使用默认 （内置）工具。

更新支持请求

提交支持请求后，您可能会收到 VMware 技术支持部门发出的电子邮件请求，要求您输出 vdm-support 或 svi-support 脚本。请回复该电子邮件，并在回复中附上脚本输出文件。

如果输出文件过大而不能作为附件 （大于或等于 10MB），请使用您的支持请求编号联系 VMware 技术支持部门，并请求提供 FTP 上传说明。您还可以更新支持请求，并将该文件粘贴至支持网站中。

更新支持请求

1 访问并登录 VMware 网站的支持页面。

2 单击 **[Support Request History （支持请求历史记录）]**，查找适用的支持请求编号。

3 更新支持请求，并附上 vdm-support 或 svi-support 脚本输出。

更多故障排除信息

以下 URL 指向的 VMware 知识库 （KB）文章包含有关 View Manager 的故障排除信息。知识库中的文章经常更新，以纳入新的故障排除信息。

- 排除最终用户的连接问题：

  http://www.vmware.com/info?id=342

- 排除池问题：

  http://www.vmware.com/info?id=343

- 排除 USB 问题：

  http://www.vmware.com/info?id=346

附录：locked.properties 文件

`locked.properties` 文件除了确定要返回到客户端的信息 （用以建立安全加密链路连接）之外，它还包含与服务器通信相关的属性。表 A-1 中描述了这些属性。

表 A-1. locked.properties – **客户端和服务器的属性**

属性	**描述**
`clientHost`	客户端与安全服务器进行通信时将采用的可外部解析的主机名。 如果未指定，会将该属性设置为 `serverName` 指定的值或者系统默认值。
`clientPort`	客户端与安全服务器进行通信时将采用的指定端口。 如果未指定，会将该属性设置为 `serverPort` 指定的值或者系统默认值。
`clientProtocol`	客户端与安全服务器进行通信时将采用的协议，此属性值可为 `http` 或 `https`。 如果未指定，会将该属性设置为 `serverProtocol` 指定的值或者系统默认值。
`serverName`	安全服务器的唯一标识。
`serverPort`	安全服务器的侦听端口。默认值为 `80`。
`serverProtocol`	安全服务器使用的协议，此属性值可为 `http` 或 `https`。 默认协议为 `http`。

默认情况下，clientHost、clientPort 和 clientProtocol 属性为安全服务器提供的默认值。服务器设置本身可使用 serverName、serverPort 和 serverProtocol 属性进行明确配置。如果已明确设置了上述值，则客户端与服务器之间的端口值和协议值应彼此关联。

如果客户端与安全服务器之间存在中间 SSL 加速器，则您可能需要指定不同的端口和协议设置。在这种情况下，clientPort 和 clientProtocol 应分别设为 443 和 https，但加速器与服务器之间的后端通信必须使用端口 80 通过 http 进行。

术语表

字母

Active Directory

指用来存储网络操作系统信息并提供服务的 Microsoft 目录服务软件。 Active Directory 可配置和管理用户和用户组，并支持管理员设置安全性策略、控制资源并在整个企业范围内部署程序。

DMZ （隔离区）

指将内部服务器连接到不受信任的大型网络 （通常指 Internet）的逻辑子网或物理子网，它可以增强安全性，并支持管理员更有效地控制访问网络资源的用户。

DNS （域名系统）

指将主机名转换为 IP 地址的 Internet 数据查询服务。也称为 "域名服务器" 或 "域名服务"。

FQDN （主机域名全称）

指包含主机名和域名的主机名。例如，在 `vmware.com` 域中， `esx1` 主机的 FQDN 为 `esx1.vmware.com`。

RDP （远程桌面协议）

指允许用户远程连接到计算机的多通道协议。

RSA SecurID

是 RSA 提供的一种产品，可使用密码和身份验证程序提供功能强大的双因素身份验证。

A

安全服务器

指在 Internet 和内部网络之间添加安全层的 View Connection Server 部署。

F

非永久桌面池

指其中的用户未分配给特定桌面的桌面池。如果用户注销桌面或桌面超时，其桌面将返回池中，以供其他用户使用。使用非永久池时，用户无法将数据或文件保存到桌面。

负载平衡

指一种用来将进程分摊至各服务器之中、以便更均匀地分散流量负载、从而避免服务器过载的技术。

G

高可用性

指一种确保操作连续性程度的系统设计方法。

管理员用户界面

指基于 Web 的管理员用户界面，可用来在 View Manager 中执行配置和管理任务。也称为 View Administrator。

H

活动会话

指 View Client 或 View Portal 用户到虚拟桌面的实时连接。它是与虚拟桌面已建立的且尚未超时的连接。

K

客户机

请参阅 "客户机操作系统"。

客户机操作系统

指在虚拟机内部运行的操作系统。

L

连接中介器

指允许远程用户与虚拟桌面连接在一起、并提供身份验证和会话管理的服务器。View Connection Server 就是一种连接中介器。

S

瘦客户端

指支持用户访问虚拟桌面、但几乎无需内存或磁盘驱动器空间的设备。应用程序软件、数据和 CPU 电源均驻留在网络计算机、而不是客户端设备中。

数据存储

指将数据中心内的基本物理存储资源组合在一起的虚拟表现形式。数据存储是虚拟机文件的存储位置（例如，物理磁盘、 RAID 或 SAN）。

X

虚拟桌面

指在虚拟机中运行的桌面操作系统。虚拟桌面与任何运行相同操作系统的其他计算机毫无区别。

Y

永久桌面池

指其中的用户已分配给特定桌面的桌面池。用户每次都登录到相同的桌面，且当用户注销时，用户数据将会保留。使用永久池时，用户可以将数据或文件保存到桌面。

Z

中介器

也称为连接中介器。 View Connection Server 就是一种连接中介器。

桌面

请参阅 “虚拟桌面”。

桌面池

指管理员为用户或用户组指定的虚拟机池。*另请参阅* “永久桌面池” 和 “非永久桌面池”。

桌面虚拟机

请参阅 “虚拟桌面”。

索引

G

H

J

K

L

O

Y

Z